Hot Issues in Data Privacy

Friday, February 1, 2019 | 8:00 am to 9:00 am &
Saturday, February 2, 2019 | 11:30 am to 12:30 pm

Program Description
Tell Me, Give Me, Protect Me, Forget Me: Relating to Customers in the Age of Consumer (Data Subject) Privacy Rights. The EU's GDPR has been in effect for almost a year, and California passed the California Consumer Privacy Act (CCPA) over the summer (which will come into effect - in some form - in 2020), both of which give new and significant rights to consumers in terms of how their data can be used. What does that mean to us, how do we operationalize it those requirements, particularly since we still don’t know exactly what the CCPA will end up requiring? What does that mean to all our cool new projects that rely on creative uses of customer data? Should we expect this to spread, or is it limited to California? Do these new laws make data breaches more or less problematic for us? And how do Internet of Things (IoT) devices and biometric identification fit in?

Lead Facilitator
Doron Goldstein, Katten Muchin Rosenman | New York, NY

Facilitators
- Kristine Holm, Twenty-First Century Fox, Inc | Los Angeles, CA
- Jadzia Pierce, Covington & Burling | Washington, D.C.
- Kathleen Scott, Wiley Rein | Washington, D.C.
- Sherrese Smith, Paul Hastings | Washington, D.C.
- S. Jenell Trigg, Lerman Senter | Washington, D.C.

Program Materials
1. Guidelines on the Right to Data Portability
2. Guidelines on Transparency under Regulation 2016/679
3. Tell Me, Give Me, Protect Me, Forget Me: Relating to Customers in the Age of Consumer (Data Subject) Privacy Rights
5. Unofficial Katten Consolidation California Consumer Privacy Act of 2018
Tell Me, Give Me, Protect Me, Forget Me:
Relating to Customers in the Age of Consumer (Data Subject) Privacy Rights
American Bar Association
January 2019

Doron S. Goldstein
Katten Muchin Rosenman LLP
Privacy Law Background

Privacy vs. Security: Privacy
- A right to know about, and exercise control over, use of data
  - “A right to be let alone”¹
- Safeguards
  - Notice, disclosure, transparency about use of data
  - Control (opt-in, opt-out) over use of data
  - Individual privacy rights
  - CCPA, GDPR, HIPAA Privacy Rule, BIPA, Breach Notification Laws
- Privacy Violation
  - Unauthorized use, disclosure, or misuse of data

Privacy vs. Security: Security
- Protection of data
- Safeguards
  - Physical, technical, administrative measures
  - Protect confidentiality, integrity, availability, [resilience] of data
  - HIPAA Security Rule, Gramm-Leach-Bliley, NYDFS
- Security Violation:
  - Data breach
    - Unauthorized access, use, disclosure, destruction

Privacy Background
- U.S. vs EU Approaches to Privacy
  - The U.S. has a (mostly) sectoral privacy regulation model.
    - No overarching, generally-applicable privacy regulation (yet!).
    - Industry-specific regulations for sectors that handle more sensitive information: financial industry (GLBA), healthcare (HIPAA), children (COPPA).

• Processing of personal data is generally permitted, unless otherwise prohibited by a specific regulation.
• Focus more generally on security than privacy.
  o The California Consumer Privacy Act of 2018 (“CCPA”) looks to change this.

Background

• U.S. vs EU Approaches to Privacy
  o The EU has a comprehensive privacy regulation model.
    ▪ Privacy is a “human right” protected by the European Convention of Human Rights and national laws.\(^2\)
    ▪ Processing of personal data is generally prohibited, unless there is a “legal basis” for such processing.\(^3\)
  o Primary focus on privacy rather than security.

• U.S. vs EU Approaches to Privacy:
  o Impact of the differing approaches:
    ▪ Inconsistencies in requirements.
      ❖ Privacy vs. security
    ▪ Implicit or explicit extraterritoriality.
    ▪ Cross-border data transfer issues.

\(^2\) Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter “GDPR”) Recital 1.

\(^3\) GDPR Art. 6.
The General Data Protection Regulation (GDPR)

What is the GDPR?

- The General Data Protection Regulation (“GDPR”) was adopted by the EU in April 2016.
  - Replaced the prior Data Protection Directive.
  - Became effective on May 25, 2018.
  - It is a “regulation” – it applies to each EU member state directly (does not need an implementing law passed by each state).

What Does the GDPR Do?

- Generally:
  - Strengthens and unifies data protection standards.
  - Expands internal compliance requirements.
  - Adds security requirements.
  - Broader scope and greater extraterritorial reach.\(^4\)
  - Increases penalties:
    - Greater of €20 million or 4% of worldwide turnover for violations of certain requirements including principles, data subjects’ rights & international transfers.\(^5\)
    - Greater of €10 million or 2% of worldwide turnover for other violations.\(^6\)

Territorial Reach

- Can reach to certain U.S. businesses and operations
- Territorial Scope:
  - Establishment of the data controller or processor in the EU:\(^7\)
    - Controller: Where decision-making occurs.\(^8\)
    - Processor: Where processing takes place.\(^9\)
  - Data subject is in the EU:
    - Offer of goods or services.

\(^5\) GDPR Art. 83(5).
\(^6\) GDPR Art. 83(4).
\(^7\) GDPR Art. 3(1)
\(^8\) GDPR Art. 4(7).
\(^9\) GDPR Art. 4(8).
Tracking of data subjects.¹⁰

**Key GDPR Terms and Concepts**

- **Data Subject**
  - A [living] identified or identifiable natural person.¹¹

- **Processing**
  - Any operation or set of operations performed upon personal data or sets of personal data, automated or otherwise, including: collection, recording, organization, structuring, use, storage, adaptation/alteration, retrieval, disclosure, combination, restriction, erasure or destruction.¹²

- **Personal data**
  - Information capable of identifying a Data Subject, including:¹³
    - Name
    - ID number
    - Location data
    - Online identifier
    - One or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of a data subject.

- **Special Categories of Data/Sensitive Data¹⁴**
  - Racial or ethnic origin
  - Political opinions, religious or philosophical beliefs
  - Trade union membership
  - Genetic and biometric data
  - Health
  - Sex life and sexual orientation
  - Note: Does not include financial data, national IDs (e.g. SSNs), children’s data.

---

¹⁰ GDPR Art. 3(2).
¹¹ GDPR Art. 4(1).
¹² GDPR Art. 4(2).
¹³ GDPR Art. 4(1).
¹⁴ GDPR Art. 9(1), 10.
- **Controller**
  - A person or entity who (alone or jointly with others) determines the purposes for which and the means by which any personal data are, or are to be, processed.\(^{15}\)

- **Processor**
  - A person or entity who processes personal data on behalf of a controller.\(^{16}\)
  - A processor that exercises independent authority would be a controller.\(^{17}\)

### Data Subject-Related Considerations

#### Transparency

- Controllers must give notice of policies, practices, and individual rights regarding processing of personal data\(^{18}\)
  - Privacy Notices or Privacy Statements.
  - “Concise, transparent, intelligible, and easily accessible form using clear and plain language.”\(^{19}\)
  - Consider layered privacy notices.\(^{20}\)
- Must provide data subjects with information regarding personal data collected about them and its processing, free of charge.\(^{21}\)

#### Purpose Limitation

- Personal data must be collected and processed only for specific, limited purposes.\(^{22}\)
  - Personal data must not be processed in a manner incompatible with those initial purposes absent subsequent notice and consent.
  - Certain additional “public interest” purposes may be permitted.\(^{23}\)
- Avoid unnecessary or unauthorized processing of personal data.

---

\(^{15}\) GDPR Art. 4(7).

\(^{16}\) GDPR Art. 4(8).

\(^{17}\) GDPR Art. 28(10).

\(^{18}\) GDPR Art. 12-14.

\(^{19}\) GDPR Art. 12(1).


\(^{21}\) GDPR Art. 12(5).

\(^{22}\) GDPR Art. 5(1)(b).

\(^{23}\) GDPR Recital 50.
Data Minimization

- Avoid excessive, unnecessary collection of personal data.
- Personal data collected must be: 24
  - Adequate;
  - Relevant; and
  - Limited to what is necessary in relation to the purposes for which the data are processed.

Data Retention

- Personal data should be stored only as long as necessary for the purposes for which it was processed 25
  - Retention period, or criteria used to determine retention period, must be disclosed to the data subject 26
- May be retained for archiving, research or statistical purposes, subject to appropriate safeguards 27

Quality and Accuracy

- Ensure personal data is accurate and up to date, as required for processing. 28
- Data subjects have the right to:
  - Obtain a copy of personal data held by a controller; 29
  - Correct, erase, or rectify incorrect information about them; 30 and
  - Restrict processing if the data subject contests the accuracy of the information. 31
- Controllers must use “all reasonable measures” to verify the identity of data subjects who request personal data and may request additional identifying information to do so. 32

---

24 GDPR Art. 5(1)(c).
25 GDPR Art. 5(1)(e).
27 GDPR Recital 156, Art. 89.
28 GDPR Art. 5(1)(d).
29 GDPR Art. 15(3).
30 GDPR Art. 16, 17.
31 GDPR Art. 18.
32 GDPR Recital 64.
The California Consumer Protection Act (CCPA)

Background

- The CCPA passed quickly to block a similar privacy ballot initiative.
  - Initiative had obtained requisite number of signatures to appear on the November 2018 election ballot
  - Backers agreed to abandon if lawmakers passed a comparable bill before June 28
  - California legislature quickly drafted and unanimously passed the CCPA before the deadline
- GDPR took years; CCPA took ~7 days
- The CCPA becomes effective January 1, 2020; AG enforcement starts July 1, 2020
  - Affected companies and organizations have approximately 14 months to prepare
- The CCPA includes a number of ambiguities, vague or superfluous provisions, redundancies, and errors (even after amendments in August):
  - Definition of “processing” refers to “personal data
  - “Personal Information” includes, for example, “biometric information” and separately “olfactory” and “thermal” information
  - Definition of publicly available information “made available from federal, state, or local government records, if any conditions associated with such information [?].”
  - The CCPA supersedes all laws and rules of any “city, county, city and county, municipality, or local agency…”
- It is still a moving target
- Amendments are forthcoming

---

33 Cal. Civ. Code, Div. 3, Part 4, Title 1.81.5 (commencing with Section 1798.100) (hereinafter “CCPA”) 1798.198(b) (law only effective if “initiative measure No. 17-0039, The Consumer Right to Privacy Act of 2018, is withdrawn”).
34 Assembly Bill No. 375, An act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy (June 28, 2018).
35 CCPA 1798.185(c), 198(a).
36 Senate Bill No. 1121, An act to amend Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.125, 1798.130, 1798.135, 1798.140, 1798.145, 1798.150, 1798.155, 1798.185, 1798.192, 1798.196, and 1798.198 of, and to add Section 1798.199 to, the Civil Code, relating to personal information, and declaring the urgency thereof, to take effect immediately (Sept. 23, 2018).
37 CCPA 1798.140(q).
38 CCPA 1798.140(o)(1).
39 CCPA 1798.140(o)(2).
40 CCPA 1798.180.
Requirement that regulation and guidance be provided by the CA Attorney General.\(^{41}\)

- Broad public participation
- Additional categories of personal data
- Updating definition of unique identifiers
- Establishing rules
- Additional regulations

**Applicability: Businesses**

- The CCPA applies to businesses (for-profit legal entity, and affiliates) that:
  - Conduct business in California;
  - Collect “consumers’” (California residents)\(^{42}\) personal information;
  - Determine the “purposes and means” of processing of personal information; and
  - Meet one or more of the following criteria:\(^{43}\)
    - Annual gross revenues in excess of $25M USD;
    - Annually obtains (by any means) for a commercial purpose the personal information of more than 50,000 households, devices, or consumers; or
    - Derives 50% or more of its annual revenue from the sale of consumer personal information.

**Applicability: Personal Information**

- Personal Information: “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”\(^{44}\)

- Includes all the usual suspects:
  - name and address
  - government identification
  - email address
  - social security number
  - financial account information

- But goes beyond the typical information under most currents state data breach laws: \(^{45}\)

---

\(^{41}\) CCPA 1798.185.

\(^{42}\) CCPA 1798.140(g).

\(^{43}\) CCPA 1798.140(c).

\(^{44}\) CCPA 1798.140(o)(1).

\(^{45}\) CCPA 1798.140(o)(1)(A), (E), (F), (K).
- Aliases, IP addresses, and online identifiers
- Browsing history, search history, information about interactions with a website, application, or advertisement
- Inferences drawn from any personal information to create a profile about a consumer
- Biometric information, such as physiological, biological, or behavioral characteristics

**Enforcement & Penalties**

- Attorney General fines for privacy violations (starting July 1, 2020)\(^{46}\)
  - Up to $7500 per intentional violation (not clear what a “violation” is yet)
- Private claims for security violations only (and only certain categories of information)\(^{47}\)
  - Statutory damages of $100-$750 per consumer per incident (or actual damages)
    - Failure to implement “reasonable” security measures results in unauthorized access of personal information and exfiltration, theft, or disclosure
    - For statutory damages, the plaintiff must provide businesses with 30 days’ notice and opportunity to cure
      - Business must actually cure the violation and certify in writing that violations have been cured and “no further violations shall occur”\(^{48}\)

---

\(^{46}\) CCPA 1798.155(b).

\(^{47}\) CCPA 1798.150.

\(^{48}\) CCPA 1798.150(b).
CCPA-GDPR Comparison: Notable Similarities

- Specific notice and disclosure requirements\(^{49}\)
- Identifying affected processing activities for compliance purposes\(^{50}\)
- Rights requests must pass through to processors/service providers\(^{51}\)
- Processors/service providers should assist controllers/businesses with compliance obligations\(^{52}\)
- De-identified data concepts are somewhat similar, although CCPA adds a “reasonableness” standard to whether information can be used to identify an individual, and the GDPR has a broader use of the concept of pseudonymization.\(^{53}\)

\(^{49}\) E.g., CCPA 1798.100(b), 130(a)(5), 135(a); GDPR Art. 12-14.

\(^{50}\) CCPA 1798.130(a)(2)-(5); GDPR Art. 30

\(^{51}\) E.g., CCPA 1798.105(c); GDPR Art. 17(2), 28(3)(e).

\(^{52}\) CCPA 1798.145(a)(3); GDPR Art. 28, 32-36.

\(^{53}\) CCPA 1798.140(h), (r); GDPR Art. 4(5).
Operational Considerations: Recordkeeping and Data Retention/Deletion

Recordkeeping Requirements

- Under the GDPR, controllers must create and retain records of at least the following: 54
  - Name and contact information for controllers and representatives
  - Purposes of processing
  - Description of categories of data subjects and categories of personal data
  - Lawful basis for processing each category of personal data
  - Categories of recipients to whom data will be disclosed and vendor agreements
  - Description of data security measures
  - Data breaches
  - Data Protection Impact Assessments

Data Retention/Deletion

- GDPR Art 5(1)(e) “storage limitation”
  - Personal data shall be:
    - “kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data are processed“
    - “personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes…”
  - Implement record retention and record deletion processes

54 GDPR Art. 30, 33(5).
Data Subject (Consumer) Rights

Data Subject (Consumer) Rights

• Transparency/Right to be Informed\textsuperscript{55}
• Access & Portability\textsuperscript{56}
• Rectification\textsuperscript{57}
• Erasure/Deletion/”Right to be Forgotten”\textsuperscript{58}
• Restriction of Processing\textsuperscript{59}
• Objection\textsuperscript{60}
• Opt-Out & Non-Discrimination (CCPA)\textsuperscript{61}
• Generally (there are exceptions, and possible extensions) must respond within 30 days (GDPR)/45 days (CCPA) of data subject request.\textsuperscript{62}

GDPR/CCPA Comparison: Data Subject Rights

• Differences
  o GDPR
    ▪ Rights are generally broader with fewer exceptions
    ▪ Additional Rights: object to/restrict processing, rectification, object to automated decisionmaking\textsuperscript{63}
  o CCPA
    ▪ Rights are generally more limited
    ▪ Additional right to opt out of sale of personal information\textsuperscript{64}
    ▪ Specifies means for exercising rights (toll-free number, opt-out button)\textsuperscript{65}

---

\textsuperscript{55} E.g., CCPA 1798.100(b), 130(a)(5), 135(a)(2); GDPR Art. 12-14.
\textsuperscript{56} CCPA 1798.100(d), 110(b), 115(b), 130(a)(2)-(5); GDPR Art. 15.
\textsuperscript{57} GDPR Art. 16.
\textsuperscript{58} CCPA 1798.105(a); GDPR Art. 17.
\textsuperscript{59} GDPR Art. 18.
\textsuperscript{60} GDPR Art. 21.
\textsuperscript{61} CCPA 1798.120(a), 125(a)(1), 135(a).
\textsuperscript{62} CCPA 1798.130(a)(2), 1798.145(g)(1); GDPR Art. 12(3).
\textsuperscript{63} GDPR Art. 18, 21, 22.
\textsuperscript{64} CCPA 1798.120.
\textsuperscript{65} CCPA 1798.130(a)(1).
Data Subject Rights: Transparency/Right to be Informed

Data Subject Rights: Transparency/Informed

- GDPR Rights of Transparency – the right to know (via Privacy Notice, other disclosure)
  - What personal data is processed;
  - For what purposes;
  - On what (lawful) basis;
  - Location of processing;
  - Sources and recipients of personal data; and
  - Right to know about data subject rights.
- Other specific requirements (automated decision-making, retention, etc.)
- CCPA rights are similar to GDPR right of transparency and purpose limitations
- Businesses subject to CCPA:
  - “shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used.”
  - “shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.”
- CCPA
  - Right to request information about personal information collected, disclosed, or sold:
    - Categories of personal information collected and “specific pieces” of personal information
      - Broad definition of “personal information” makes responding to such requests challenging
  - Certain specific additional requirements
    - Sources of personal information

---

66 GDPR Art. 12-14.
67 CCPA 1798.100(b).
68 Id.
69 CCPA 1798.100(a), 110(c)(5).
70 CCPA 1798.140(o).
71 CCPA 1798.110(a)(2), (c)(2)
- Purpose for collection/sale/disclosure\textsuperscript{72}

- CCPA - Mandates Updating Privacy Notice/Policy every 12 months\textsuperscript{73}
  - Disclose whether the business sells personal information
  - Identify consumer rights and describe how they can be exercised
  - List the categories of personal information collected in the last 12 months
  - List the categories of personal information sold in the last 12 months
  - Describe whether personal information was disclosed for business purposes, and the categories disclosed in the last 12 months
  - Other items (financial incentives for sale of personal information, etc.)\textsuperscript{74}

**Data Subject Rights: Access & Portability**

- GDPR Right of Access\textsuperscript{75}
  - Right to access and receive a copy of personal data concerning them
    - Free of charge except for repetitive, unfounded, or excessive requests
  - Right to receive basic information about the controller and reasons for processing, and other relevant information

- GDPR Right of Data Portability\textsuperscript{76}
  - Right to receive copy of personal data in a commonly-used machine-readable format so that it can be transferred from one controller to another

- Under the CCPA, businesses must deliver, free of charge and up to twice every 12 months, the personal information the business holds about the consumer.\textsuperscript{77}
  - “Categories and specific pieces” of personal information collected\textsuperscript{78}
  - Broad definition of personal information means that responses to these requests can be extensive\textsuperscript{79}

\textsuperscript{72} CCPA 1798.100(b), 110(a)(3), (c)(3)
\textsuperscript{73} CCPA 1798.130(a)(5).
\textsuperscript{74} CCPA 1798.125(b)(2).
\textsuperscript{75} GDPR Art. 15.
\textsuperscript{76} GDPR Art. 20.
\textsuperscript{77} CCPA 1798.100(d) 110(b), 115(b),130(a)(2)-(5).
\textsuperscript{78} CCPA 1798.100(a), 110(c)(5).
\textsuperscript{79} CCPA 1798.140(o).
The CCPA requires that if information is provided electronically, “to the extent feasible,” the information must be provided in a “readily usable format” that allows the consumer to transmit the information to another entity “without hindrance.”

Must provide two or more methods of submitting requests for information:
- One must be a toll-free telephone number
- Another must be a “Web site address” if the business maintains an “Internet Web site”

CCPA only covers the 12-month period preceding the request

**Data Subject Rights: Erasure/Deletion – “Right to be Forgotten”**

**Data Subject Rights: Erasure/Deletion**

- GDPR Right of Erasure (Right to be Forgotten)
  - Right to have data deleted in certain situations, including:
    - Personal data is no longer necessary for its original purpose;
    - Withdrawn consent to processing; or
    - Data subject has objected to the processing.
- If there is a lawful basis for an organization to hold personal data, it does not need to be deleted.
- Right to be Forgotten is an extension, where information is public, and includes notification of other controllers
- Under the CCPA, Consumers can request deletion of certain personal information collected by the business.
  - Significant exceptions, including:
    - Comply with legal obligations, exercise free speech or other legal rights
    - Carry out transactions, perform under contracts, or provide goods/services
    - Detect security incidents, protect against fraudulent, malicious, deceptive activity

---

80 CCPA 1798.130(a)(2).
81 CCPA 1798.130(a)(1)
82 CCPA 1798.130(a)(2)
83 GDPR Art. 17(1)(a)-(c).
84 GDPR Art. 17(1)(b).
85 GDPR Art. 17(2).
86 CCPA 1798.105.
87 CCPA 1798.105(d).
Enable “solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer’s relationship with the business”

Internal use in a lawful manner that is compatible with the context in which the consumer provided the information

**GDPR Data Subject Rights: Rectification, Restriction & Objection to Processing**

**Data Subject Rights: GDPR-Specific**

- Right to Rectification
  - Right to have “inaccurate” personal data corrected
  - Right to have “incomplete” personal data “completed” 88

- Right to restrict processing
  - Personal data may only be held and used for limited purposes in similar situations. 89

- Right to object to processing
  - Includes uses for direct marketing and profiling/automated decision making 90

**CCPA Data Subject Rights: Right to Opt-Out / Right to Non-Discrimination**

**Data Subject Rights: CCPA-Specific**

- Right to Opt-Out:
  - Right to restrict a business from *selling* personal information to a third party (*i.e.*, Right to Opt-Out). 91
    - Sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means
    - A consumer’s personal information for *monetary* or *other valuable consideration*. 92
  - May authorize another person to opt out on the consumer’s behalf. 93

---

88 GDPR Art. 16.

89 GDPR Art. 18.

90 GDPR Art. 21.

91 CCPA 1798.120.

92 CCPA 1798.140(t).

93 CCPA 1798.135(a)(c).
• Must honor consumer opt-out requests for at least 12 months before re-seeking consumer consent.94

• “**Do Not Sell My Personal Information**” link must be placed prominently on the homepage for businesses that sell personal information.95
  
  o CA Attorney General tasked with creating rules and procedures for opt-out requirements.96
  
  o Sale of personal information for consumers under 16 requires opt-in consent.97
    ▪ Consumers under 13 requires parental/guardian consent
    ▪ “A business that *willfully disregards* the consumer’s age shall be deemed to have had actual knowledge of the consumer’s age.”98
    ▪ Inconsistent with federal law (COPPA)99

• Right to Non-Discrimination:
  
  o CCPA prohibits a business from discriminating against consumers that exercise their rights under the new law.100

• Including **but not limited** to:
  
  o Denying goods/services
  
  o Charging different prices for goods/services
  
  o Providing a different level quality for goods/services
  
  o Suggesting that the consumer will receive a different price or quality for goods/services101

• Right to Non-Discrimination:
  
  o Differential pricing or quality is allowed where it is “*reasonably related* to the value provided to the consumer . . . .”
  
  o Differential pricing or quality is allowed where it is “*directly related* to the value provided to the consumer . . . .”102

---

94 CCPA 1798.135(a)(5).
95 CCPA 1798.135(a)(1)-(2).
96 CCPA 1798.185(a)(4).
97 CCPA 1798.120(c).
98 Id.
99 15 USC 6501 *et seq.*
100 CCPA 1798.125(a).
101 Id.
102 1798.125(a)(2), (b)(1).
- Financial incentive programs are also allowed: 103
  - If disclosed;
  - If consumer provides opt-in consent (revocable at any time); and
  - Are not “unjust, unreasonable, coercive, or usurious in nature.”
- This one is a particular mess, and we await amendments to explain.

103 CCPA 1798.125(b).
Guidelines on the right to data portability

Adopted on 13 December 2016
As last Revised and adopted on 5 April 2017

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental rights and rule of law) of the European Commission, Directorate General Justice and Consumers, B-1049 Brussels, Belgium, Office No MO59 05/35

Website: http://ec.europa.eu/justice/data-protection/index_en.htm
TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive summary</td>
<td>3</td>
</tr>
<tr>
<td>I. Introduction</td>
<td>3</td>
</tr>
<tr>
<td>II. What are the main elements of data portability?</td>
<td>4</td>
</tr>
<tr>
<td>III. When does data portability apply?</td>
<td>8</td>
</tr>
<tr>
<td>IV. How do the general rules governing the exercise of data subject</td>
<td>13</td>
</tr>
<tr>
<td>rights apply to data portability?</td>
<td></td>
</tr>
<tr>
<td>V. How must the portable data be provided?</td>
<td>15</td>
</tr>
</tbody>
</table>
Executive summary

Article 20 of the GDPR creates a new right to data portability, which is closely related to the right of access but differs from it in many ways. It allows for data subjects to receive the personal data that they have provided to a controller, in a structured, commonly used and machine-readable format, and to transmit those data to another data controller. The purpose of this new right is to empower the data subject and give him/her more control over the personal data concerning him or her.

Since it allows the direct transmission of personal data from one data controller to another, the right to data portability is also an important tool that will support the free flow of personal data in the EU and foster competition between controllers. It will facilitate switching between different service providers, and will therefore foster the development of new services in the context of the digital single market strategy.

This opinion provides guidance on the way to interpret and implement the right to data portability as introduced by the GDPR. It aims at discussing the right to data portability and its scope. It clarifies the conditions under which this new right applies taking into account the legal basis of the data processing (either the data subject’s consent or the necessity to perform a contract) and the fact that this right is limited to personal data provided by the data subject. The opinion also provides concrete examples and criteria to explain the circumstances in which this right applies. In this regard, WP29 considers that the right to data portability covers data provided knowingly and actively by the data subject as well as the personal data generated by his or her activity. This new right cannot be undermined and limited to the personal information directly communicated by the data subject, for example, on an online form.

As a good practice, data controllers should start developing the means that will contribute to answer data portability requests, such as download tools and Application Programming Interfaces. They should guarantee that personal data are transmitted in a structured, commonly used and machine-readable format, and they should be encouraged to ensure the interoperability of the data format provided in the exercise of a data portability request.

The opinion also helps data controllers to clearly understand their respective obligations and recommends best practices and tools that support compliance with the right to data portability. Finally, the opinion recommends that industry stakeholders and trade associations work together on a common set of interoperable standards and formats to deliver the requirements of the right to data portability.

I. Introduction

Article 20 of the General Data Protection Regulation (GDPR) introduces a new right of data portability. This right allows for data subjects to receive the personal data that they have provided to a data controller, in a structured, commonly used and machine-readable format, and to transmit those data to another data controller without hindrance. This right, which applies subject to certain conditions, supports user choice, user control and user empowerment.
Individuals making use of their right of access under the Data Protection Directive 95/46/EC were constrained by the format chosen by the data controller when providing the requested information. **The new right to data portability aims to empower data subjects regarding their own personal data, as it facilitates their ability to move, copy or transmit personal data easily from one IT environment to another** (whether to their own systems, the systems of trusted third parties or those of new data controllers).

By affirming individuals’ personal rights and control over the personal data concerning them, data portability also represents an opportunity to “re-balance” the relationship between data subjects and data controllers.¹

Whilst the right to personal data portability may also enhance competition between services (by facilitating service switching), the GDPR is regulating personal data and not competition. In particular, article 20 does not limit portable data to those which are necessary or useful for switching services².

Although data portability is a new right, other types of portability already exist or are being discussed in other areas of legislation (e.g. in the contexts of contract termination, communication services roaming and trans-border access to services³). Some synergies and even benefits to individuals may emerge between the different types of portability if they are provided in a combined approach, even though analogies should be treated cautiously.

This Opinion provides guidance to data controllers so that they can update their practices, processes and policies, and clarifies the meaning of data portability in order to enable data subjects to efficiently use their new right.

### II. What are the main elements of data portability?

The GDPR defines the right of data portability in Article 20 (1) as follows:

> The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the data have been provided […]

- **A right to receive personal data**

Firstly, data portability is a right of the data subject to receive a subset of the personal data processed by a data controller concerning him or her, and to store those data for further personal use. Such storage can be on a private device or on a private cloud, without necessarily transmitting the data to another data controller.

---

¹ The primary aim of data portability is enhancing individual’s control over their personal data and making sure they play an active role in the data ecosystem.

² For example, this right may allow banks to provide additional services, under the user’s control, using personal data initially collected as part of an energy supply service.


---
In this regard, data portability complements the right of access. One specificity of data portability lies in the fact that it offers an easy way for data subjects to manage and reuse personal data themselves. These data should be received “in a structured, commonly used and machine-readable format”. For example, a data subject might be interested in retrieving his current playlist (or a history of listened tracks) from a music streaming service, to find out how many times he listened to specific tracks, or to check which music he wants to purchase or listen to on another platform. Similarly, he may also want to retrieve his contact list from his webmail application, for example, to build a wedding list, or get information about purchases using different loyalty cards, or to assess his or her carbon footprint.

- **A right to transmit personal data from one data controller to another data controller**

Secondly, Article 20(1) provides data subjects with the right to transmit personal data from one data controller to another data controller “without hindrance”. Data can also be transmitted directly from one data controller to another on request of the data subject and where it is technically feasible (Article 20(2)). In this respect, recital 68 encourages data controllers to develop interoperable formats that enable data portability but without creating an obligation for controllers to adopt or maintain processing systems which are technically compatible. The GDPR does, however, prohibit controllers from establishing barriers to the transmission.

In essence, this element of data portability provides the ability for data subjects not just to obtain and reuse, but also to transmit the data they have provided to another service provider (either within the same business sector or in a different one). In addition to providing consumer empowerment by preventing “lock-in”, the right to data portability is expected to foster opportunities for innovation and sharing of personal data between data controllers in a safe and secure manner, under the data subject’s control. Data portability can promote the controlled and limited sharing by users of personal data between organisations and thus enrich services and customer experiences. Data portability may facilitate transmission and reuse of personal data concerning users among the various services they are interested in.

---

4 In these cases, the processing performed on the data by the data subject can either fall within the scope of household activities, when all the processing is performed under the sole control of the data subject, or it can be handled by another party, on the data subject’s behalf. In the latter case, the other party should be considered as data controller, even for the sole purpose of personal data storage, and must comply with the principles and obligations laid down in the GDPR.

5 See also section V.

6 As a consequence, special attention should be paid to the format of the transmitted data, so as to guarantee that the data can be re-used, with little effort, by the data subject or another data controller. See also section V.

7 See several experimental applications in Europe, for example MiData in the United Kingdom, MesInfos / SelfData by FING in France.

8 The so-called quantified self and IoT industries have shown the benefit (and risks) of linking personal data from different aspects of an individual’s life such as fitness, activity and calorie intake to deliver a more complete picture of an individual’s life in a single file.
- **Controllership**

Data portability guarantees the right to receive personal data and to process them, according to the data subject’s wishes.

Data controllers answering data portability requests, under the conditions set forth in Article 20, are not responsible for the processing handled by the data subject or by another company receiving personal data. They act on behalf of the data subject, including when the personal data are directly transmitted to another data controller. In this respect, the data controller is not responsible for compliance of the receiving data controller with data protection law, considering that it is not the sending data controller that chooses the recipient. At the same time the controller should set safeguards to ensure they genuinely act on the data subject’s behalf. For example, they can establish procedures to ensure that the type of personal data transmitted are indeed those that the data subject wants to transmit. This could be done by obtaining confirmation from the data subject either before transmission or earlier on when the original consent for processing is given or the contract is finalised.

Data controllers answering a data portability request have no specific obligation to check and verify the quality of the data before transmitting it. Of course, these data should already be accurate, and up to date, according to the principles stated in Art 5(1) of the GDPR. Moreover, data portability does not impose an obligation on the data controller to retain personal data for longer than is necessary or beyond any specified retention period.

Importantly, there is no additional requirement to retain data beyond the otherwise applicable retention periods, simply to serve any potential future data portability request.

Where the personal data requested are processed by a data processor, the contract concluded in accordance with Article 28 of the GDPR must include the obligation to assist “the controller by appropriate technical and organisational measures, (...) to respond to requests for exercising the data subject’s rights”. The data controller should therefore implement specific procedures in cooperation with its data processors to answer data portability requests. In case of a joint controllership, a contract should allocate clearly the responsibilities between each data controller regarding the processing of data portability requests.

In addition, a receiving data controller is responsible for ensuring that the portable data provided are relevant and not excessive with regard to the new data processing. For example, in the case of a data portability request made to a webmail service, where the request is used by the data subject to obtain emails and send them to a secured archive platform, the new data controller does not need to process the contact details of the data subject’s correspondents. If this information is not relevant with regard to the purpose of the new processing, it should not be kept and processed. In any case, receiving data controllers are not obliged to accept and process personal data transmitted following a data portability request. Similarly, where a data subject requests the transmission of details of his or her bank transactions to a service that assists in managing his or her budget, the receiving data controller does not need to accept all the data, or to retain all the details of the transactions once they have been labelled for the

---

9 The right to data portability is not limited to personal data that are useful and relevant for similar services provided by competitors of the data controller.

10 In the example above, if the data controller does not retain a record of songs played by a user then this personal data cannot be included within a data portability request.

11 i.e. that receives personal data following a data portability request made by the data subject to another data controller.
purposes of the new service. In other words, the data accepted and retained should only be that which is necessary and relevant to the service being provided by the receiving data controller.

A “receiving” organization becomes a new data controller regarding these personal data and must respect the principles stated in Article 5 of the GDPR. Therefore, the “new” receiving data controller must clearly and directly state the purpose of the new processing before any request for transmission of the portable data in accordance with the transparency requirements set out in Article 14. As for any other data processing performed under its responsibility, the data controller should apply the principles laid down in Article 5, such as lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, integrity and confidentiality, storage limitation and accountability.

Data controllers holding personal data should be prepared to facilitate their data subject’s right to data portability. Data controllers can also choose to accept data from a data subject, but are not obliged to.

- Data portability vs. other rights of data subjects

When an individual exercises his or her right to data portability he or she does so without prejudice to any other right (as is the case with any other rights in the GDPR). A data subject can continue to use and benefit from the data controller’s service even after a data portability operation. Data portability does not automatically trigger the erasure of the data from the systems of the data controller, and does not affect the original retention period applying to the data which have been transmitted. The data subject can exercise his or her rights as long as the data controller is still processing the data.

Equally, if the data subject wants to exercise his or her right to erasure (“right to be forgotten” under Article 17), data portability cannot be used by a data controller as a way of delaying or refusing such erasure.

Should a data subject discover that personal data requested under the right to data portability does not fully address his or her request, any further request for personal data under a right of access should be fully complied with, in accordance with Article 15 of the GDPR.

Furthermore, where a specific European or Member State law in another field also provides for some form of portability of the data concerned, the conditions laid down in these specific laws must also be taken into account when satisfying a data portability request under the GDPR. First, if it is clear from the request made by the data subject that his or her intention is not to exercise rights under the GDPR, but rather, to exercise rights under sectorial legislation.

---

12 In addition, the new data controller should not process personal data, which are not relevant, and the processing must be limited to what is necessary for the new purposes, even if the personal data are part of a more global data-set transmitted through a portability process. Personal data, which are not necessary to achieve the purpose of the new processing, should be deleted as soon as possible.

13 Once received by the data controller, the personal data sent as part of the right to data portability can be considered as “provided by” the data subject and be re-transmitted according to the right to data portability, to the extent that the other conditions applicable to this right (i.e. the legal basis of the processing, …) are met.

14 as stated in Article 17 of the GDPR
only, then the GDPR’s data portability provisions will not apply to this request. If, on the other hand, the request is aimed at portability under the GDPR, the existence of such specific legislation does not override the general application of the data portability principle to any data controller, as provided by the GDPR. Instead, it must be assessed, on a case by case basis, how, if at all, such specific legislation may affect the right to data portability.

III. When does data portability apply?

- Which processing operations are covered by the right to data portability?

Compliance with the GDPR requires data controllers to have a clear legal basis for the processing of personal data.

In accordance with Article 20(1)(a) of the GDPR, in order to fall under the scope of data portability, processing operations must be based:

- either on the data subject’s consent (pursuant to Article 6(1)(a), or pursuant to Article 9(2)(a) when it comes to special categories of personal data);
- or, on a contract to which the data subject is a party pursuant to Article 6(1)(b).

As an example, the titles of books purchased by an individual from an online bookstore, or the songs listened to via a music streaming service are examples of personal data that are generally within the scope of data portability, because they are processed on the basis of the performance of a contract to which the data subject is a party.

The GDPR does not establish a general right to data portability for cases where the processing of personal data is not based on consent or contract. For example, there is no obligation for financial institutions to answer a data portability request concerning personal data processed as part of their obligations obligation to prevent and detect money laundering and other financial crimes; equally, data portability does not cover professional contact details processed in a business to business relationship in cases where the processing is neither based on the consent of the data subject nor on a contract to which he or she is a party.

When it comes to employees’ data, the right to data portability typically applies only if the processing is based on a contract to which the data subject is a party. In many cases, consent will not be considered freely given in this context, due to the imbalance of power between the

15 For example, if the data subject’s request aims specifically at providing access to his banking account history to an account information service provider, for the purposes stated in the Payment Services Directive 2 (PSD2) such access should be granted according to the provisions of this directive.

16 See recital 68 and Article 20(3) of the GDPR. Article 20(3) and Recital 68 provide that data portability does not apply when the data processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, or when a data controller is exercising its public duties or complying with a legal obligation. Therefore, there is no obligation for data controllers to provide for portability in these cases. However, it is a good practice to develop processes to automatically answer portability requests, by following the principles governing the right to data portability. An example of this would be a government service providing easy downloading of past personal income tax filings. For data portability as a good practice in case of processing based on the legal ground of necessity for a legitimate interest and for existing voluntary schemes, see pages 47 & 48 of WP29 Opinion 6/2014 on legitimate interests (WP217).
employer and employee. Some HR processings instead are based on the legal ground of legitimate interest, or are necessary for compliance with specific legal obligations in the field of employment. In practice, the right to data portability in an HR context will undoubtedly concern some processing operations (such as pay and compensation services, internal recruitment) but in many other situations a case by case approach will be needed to verify whether all conditions applying to the right to data portability are met.

Finally, the right to data portability only applies if the data processing is “carried out by automated means”, and therefore does not cover most paper files.

- **What personal data must be included?**

Pursuant to Article 20(1), to be within the scope of the right to data portability, data must be:
- personal data concerning him or her, and
- which he or she has *provided* to a data controller.

Article 20(4) also states that compliance with this right shall not adversely affect the rights and freedoms of others.

**First condition: personal data concerning the data subject**

Only personal data is in scope of a data portability request. Therefore, any data that is anonymous or does not concern the data subject, will not be in scope. However, pseudonymous data that can be clearly linked to a data subject (e.g. by him or her providing the respective identifier, cf. Article 11 (2)) is within the scope.

In many circumstances, data controllers will process information that contains the personal data of several data subjects. Where this is the case, data controllers should not take an overly restrictive interpretation of the sentence “personal data concerning the data subject”. As an example, telephone, interpersonal messaging or VoIP records may include (in the subscriber’s account history) details of third parties involved in incoming and outgoing calls. Although records will therefore contain personal data concerning multiple people, subscribers should be able to have these records provided to them in response to data portability requests, because the records are (also) concerning the data subject. However, where such records are then transmitted to a new data controller, this new data controller should not process them for any purpose which would adversely affect the rights and freedoms of the third-parties (see below: third condition).

**Second condition: data provided by the data subject**

The second condition narrows the scope to data “provided by” the data subject.

There are many examples of personal data, which will be knowingly and actively “provided by” the data subject such as account data (e.g. mailing address, user name, age) submitted via online forms. Nevertheless, data “provided by” the data subject also result from the observation of his activity. As a consequence, the WP29 considers that to give its full value to this new right, “provided by” should also include the personal data that are observed from the

---

17 As the WP29 outlined in its Opinion 8/2001 of 13 September 2001 (WP48).
activities of users such as raw data processed by a smart meter or other types of connected objects, activity logs, history of website usage or search activities.

This latter category of data does not include data that are created by the data controller (using the data observed or directly provided as input) such as a user profile created by analysis of the raw smart metering data collected.

A distinction can be made between different categories of data, depending on their origin, to determine if they are covered by the right to data portability. The following categories can be qualified as “provided by the data subject”:

- **Data actively and knowingly provided by the data subject** (for example, mailing address, user name, age, etc.)

- **Observed data provided by the data subject by virtue of the use of the service or the device.** They may for example include a person’s search history, traffic data and location data. It may also include other raw data such as the heartbeat tracked by a wearable device.

In contrast, inferred data and derived data are created by the data controller on the basis of the data “provided by the data subject”. For example, the outcome of an assessment regarding the health of a user or the profile created in the context of risk management and financial regulations (e.g. to assign a credit score or comply with anti-money laundering rules) cannot in themselves be considered as “provided by” the data subject. Even though such data may be part of a profile kept by a data controller and are inferred or derived from the analysis of data provided by the data subject (through his actions for example), these data will typically not be considered as “provided by the data subject” and thus will not be within scope of this new right.

In general, given the policy objectives of the right to data portability, the term “provided by the data subject” must be interpreted broadly, and should exclude “inferred data” and “derived data”, which include personal data that are created by a service provider (for example, algorithmic results). A data controller can exclude those inferred data but should include all other personal data provided by the data subject through technical means provided by the controller.

Thus, the term “provided by” includes personal data that relate to the data subject activity or result from the observation of an individual’s behaviour, but does not include data resulting from subsequent analysis of that behaviour. By contrast, any personal data which have been

---

19 By being able to retrieve the data resulting from observation of his or her activity, the data subject will also be able to get a better view of the implementation choices made by data controller as to the scope of observed data and will be in a better situation to choose what data he or she is willing to provide to get a similar service, and be aware of the extent to which his or her right to privacy is respected.

20 Nevertheless, the data subject can still use his or her “right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data” as well as information about “the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject”, according to Article 15 of the GDPR (which refers to the right of access).

21 This includes all data observed about the data subject during the activities for the purpose of which the data are collected, such as a transaction history or access log. Data collected through the tracking and recording of the data subject (such as an app recording heartbeat or technology used to track browsing behaviour) should also be considered as “provided by” him or her even if the data are not actively or consciously transmitted.
created by the data controller as part of the data processing, e.g. by a personalisation or recommendation process, by user categorisation or profiling are data which are derived or inferred from the personal data provided by the data subject, and are not covered by the right to data portability.

**Third condition: the right to data portability shall not adversely affect the rights and freedoms of others**

**With respect to personal data concerning other data subjects:**

The third condition is intended to avoid the retrieval and transmission of data containing the personal data of other (non-consenting) data subjects to a new data controller in cases where these data are likely to be processed in a way that would adversely affect the rights and freedoms of the other data subjects (Article 20(4) of the GDPR)\(^{22}\).

Such an adverse effect would occur, for instance, if the transmission of data from one data controller to another, would prevent third parties from exercising their rights as data subjects under the GDPR (such as the rights to information, access, etc.).

The data subject initiating the transmission of his or her data to another data controller, either gives consent to the new data controller for processing or enters into a contract with that controller. Where personal data of third parties are included in the data set another legal basis for the processing must be identified. For example, a legitimate interest may be pursued by the data controller under Article 6(1)(f), in particular when the purpose of the data controller is to provide a service to the data subject that allows the latter to process personal data for a purely personal or household activity. The processing operations initiated by the data subject in the context of personal activity that concern and potentially impact third parties remain under his or her responsibility, to the extent that such processing is not, in any manner, decided by the data controller.

For example, a webmail service may allow the creation of a directory of a data subject’s contacts, friends, relatives, family and broader environment. Since these data relate to (and are created by) the identifiable individual that wishes to exercise his right to data portability, data controllers should transmit the entire directory of incoming and outgoing e-mails to that data subject.

Similarly, a data subject’s bank account can contain personal data relating to the transactions not just of the account holder but also those of other individuals (e.g., if they have transferred money to the account holder). The rights and freedoms of those third parties are unlikely to be adversely affected by the transmission of the bank account information to the account holder once a portability request is made—provided that in both examples the data are used for the same purpose (i.e., a contact address only used by the data subject or a history of the data subject’s bank account.

Conversely, the rights and freedoms of third parties will not be respected if the new data controller uses the personal data for other purposes, e.g. if the receiving data controller uses

\(^{22}\) Recital 68 provides that “where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation.”
personal data of other individuals within the data subject’s contact directory for marketing purposes.

Therefore, to prevent adverse effects on the third parties involved, the processing of such personal data by another controller is allowed only to the extent that the data are kept under the sole control of the requesting user and is only managed for purely personal or household needs. A receiving ‘new’ data controller (to whom the data can be transmitted at the request of the user) may not use the transmitted third party data for his own purposes e.g. to propose marketing products and services to those other third party data subjects. For example, this information should not be used to enrich the profile of the third party data subject and rebuild his social environment, without his knowledge and consent. Neither can it be used to retrieve information about such third parties and create specific profiles, even if their personal data are already held by the data controller. Otherwise, such processing is likely to be unlawful and unfair, especially if the third parties concerned are not informed and cannot exercise their rights as data subjects.

Furthermore, it is a leading practice for all data controllers (both the “sending” and “receiving” parties) to implement tools to enable data subjects to select the relevant data they wish to receive and transmit and exclude, where relevant, data of other individuals. This will further assist in reducing the risks for third parties whose personal data may be ported.

Additionally, the data controllers should implement consent mechanisms for other data subjects involved, to ease data transmission for those cases where such parties are willing to consent, e.g. if they also want to move their data to some other data controller. Such a situation might arise, for example, with social networks, but it is up to data controllers to decide on the leading practice to follow.

With respect to data covered by intellectual property and trade secrets:
The rights and freedoms of others are mentioned in Article 20(4). While not directly related to portability, this can be understood as “including trade secrets or intellectual property and in particular the copyright protecting the software. However, even though these rights should be considered before answering a data portability request, “the result of those considerations should not be a refusal to provide all information to the data subject”. Furthermore, the data controller should not reject a data portability request on the basis of the infringement of another contractual right (for example, an outstanding debt, or a trade conflict with the data subject).

The right to data portability is not a right for an individual to misuse the information in a way that could be qualified as an unfair practice or that would constitute a violation of intellectual property rights.

A potential business risk cannot, however, in and of itself serve as the basis for a refusal to answer the portability request and data controllers can transmit the personal data provided by data subjects in a form that does not release information covered by trade secrets or intellectual property rights.

---

23 A social networking service should not enrich the profile of its members by using personal data transmitted by a data subject as part of his right to data portability, without respecting the principle of transparency and also making sure they rely on an appropriate legal basis regarding this specific processing.
IV. How do the general rules governing the exercise of data subject rights apply to data portability?

- What prior information should be provided to the data subject?

In order to comply with the new right to data portability, data controllers must inform data subjects of the existence of the new right to portability. Where the personal data concerned are directly collected from the data subject, this must happen “at the time where personal data are obtained”. If the personal data have not been obtained from the data subject, the data controller must provide the information as required by Articles 13(2)(b) and 14(2)(c).

“When the personal data have not been obtained from the data subject”, Article 14(3) requires the information to be provided within a reasonable time not exceeding one month after obtaining the data, during first communication with the data subject, or when disclosure is made to third parties.24

When providing the required information data controllers must ensure that they distinguish the right to data portability from other rights. Therefore, WP29 recommends in particular that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability.

In addition, the Working Party recommends that data controllers always include information about the right to data portability before data subjects close any account they may have. This allows users to take stock of their personal data, and to easily transmit the data to their own device or to another provider before a contract is terminated.

Finally, as leading practice for “receiving” data controllers, the WP29 recommends that data subjects are provided with complete information about the nature of personal data which are relevant for the performance of their services. In addition to underpinning fair processing, this allows users to limit the risks for third parties, and also any other unnecessary duplication of personal data even where no other data subjects are involved.

- How can the data controller identify the data subject before answering his request?

There are no prescriptive requirements to be found in the GDPR on how to authenticate the data subject. Nevertheless, Article 12(2) of the GDPR states that the data controller shall not refuse to act on request of a data subject for exercising his or her rights (including the right to data portability) unless it is processing personal data for a purpose that does not require the identification of a data subject and it can demonstrate that it is not able to identify the data subject. However, as per Article 11(2), in such circumstances the data subject can provide more information to enable his or her identification. Additionally, Article 12(6) provides that where a data controller has reasonable doubts about the identity of a data subject, it can request further information to confirm the data subject’s identity. Where a data subject provides additional information enabling his or her identification, the data controller shall not refuse to act on the request. Where information and data collected online is linked to pseudonyms or unique identifiers, data controllers can implement appropriate procedures.

24 Article 12 requires that data controllers provide “any communications […] in a concise, transparent, intelligible, and easily assessable form, using clear and plain language, in particular for any information addressed specifically to a child.”
enabling an individual to make a data portability request and receive the data relating to him or her. In any case, data controllers must implement an authentication procedure in order to strongly ascertain the identity of the data subject requesting his or her personal data or more generally exercising the rights granted by the GDPR.

These procedures often already exist. The data subjects are often already authenticated by the data controller before entering into a contract or collecting his or her consent to the processing. As a consequence, the personal data used to register the individual concerned by the processing can also be used as evidence to authenticate the data subject for portability purposes.

While in these cases, the data subjects’ prior identification may require a request for proof of their legal identity, such verification may not be relevant to assess the link between the data and the individual concerned, since such a link is not related with the official or legal identity. In essence, the ability for the data controller to request additional information to assess one’s identity cannot lead to excessive demands and to the collection of personal data which are not relevant or necessary to strengthen the link between the individual and the personal data requested.

In many cases, such authentication procedures are already in place. For example, usernames and passwords are often used to allow individuals to access their data in their email accounts, social networking accounts, and accounts used for various other services, some of which individuals choose to use without revealing their full name and identity.

If the size of data requested by the data subject makes transmission via the internet problematic, rather than potentially allowing for an extended time period of a maximum of three months to comply with the request, the data controller may also need to consider alternative means of providing the data such as using streaming or saving to a CD, DVD or other physical media or allowing for the personal data to be transmitted directly to another data controller (as per Article 20(2) of the GDPR where technically feasible).

- **What is the time limit imposed to answer a portability request?**

Article 12(3) requires that the data controller provides “information on action taken” to the data subject “without undue delay” and in any event “within one month of receipt of the request”. This one month period can be extended to a maximum of three months for complex cases, provided that the data subject has been informed about the reasons for such delay within one month of the original request.

Data controllers operating information society services are likely to be better equipped to be able to comply with requests within a very short time period. To meet user expectations, it is a good practice to define the timeframe in which a data portability request can typically be answered and communicate this to data subjects.

Data controllers who refuse to answer a portability request shall, pursuant to Article 12(4), inform the data subject “the reasons for not taking action and on the possibility of lodging a

---

25 For example, when the data processing is linked to a user account, providing the relevant login and password might be sufficient to identify the data subject.

26 Article 12(3): “The controller shall provide information on action taken on a request”. 
complaint with a supervisory authority and seeking a judicial remedy”, no later than one month after receiving the request.

Data controllers must respect the obligation to respond within the given terms, even if it concerns a refusal. In other words, the data controller cannot remain silent when it is asked to answer a data portability request.

- In which cases can a data portability request be rejected or a fee charged?

Article 12 prohibits the data controller from charging a fee for the provision of the personal data, unless the data controller can demonstrate that the requests are manifestly unfounded or excessive, “in particular because of their repetitive character”. For information society services that specialise in automated processing of personal data, implementing automated systems such as Application Programming Interfaces (APIs)\(^\text{27}\) can facilitate the exchanges with the data subject, hence lessen the potential burden resulting from repetitive requests. Therefore, there should be very few cases where the data controller would be able to justify a refusal to deliver the requested information, even regarding multiple data portability requests.

In addition, the overall cost of the processes created to answer data portability requests should not be taken into account to determine the excessiveness of a request. In fact, Article 12 of the GDPR focuses on the requests made by one data subject and not on the total number of requests received by a data controller. As a result, the overall system implementation costs should neither be charged to the data subjects, nor be used to justify a refusal to answer portability requests.

V. How must the portable data be provided?

- What are the expected means the data controller should implement for data provision?

Article 20(1) of the GDPR provides that data subjects have the right to transmit the data to another controller without hindrance from the controller to which the personal data have been provided.

Such hindrance can be characterised as any legal, technical or financial obstacles placed by data controller in order to refrain or slow down access, transmission or reuse by the data subject or by another data controller. For example, such hindrance could be: fees asked for delivering data, lack of interoperability or access to a data format or API or the provided format, excessive delay or complexity to retrieve the full dataset, deliberate obfuscation of the dataset, or specific and undue or excessive sectorial standardization or accreditation demands\(^\text{28}\).

Article 20(2) also places obligations on data controllers for transmitting the portable data directly to other data controllers “when technically feasible”.

\(^{27}\) Application Programming Interface (API) means the interfaces of applications or web services made available by data controllers so that other systems or applications can link and work with their systems.

\(^{28}\) Some legitimate obstacles might arise, as the ones, which are related to the rights and freedoms of others mentioned in Article 20(4), or the ones that relate to the security of the controllers’ own systems. It shall be the responsibility of the data controller to justify why such obstacles would be legitimate and why they do not constitute a hindrance in the meaning of Article 20(1).
The technical feasibility of transmission from data controller to data controller, under the control of the data subject, should be assessed on a case by case basis. Recital 68 further clarifies the limits of what is “technically feasible”, indicating that “it should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible”.

Data controllers are expected to transmit personal data in an interoperable format, although this does not place obligations on other data controllers to support these formats. Direct transmission from one data controller to another could therefore occur when communication between two systems is possible, in a secured way\(^{29}\), and when the receiving system is technically in a position to receive the incoming data. If technical impediments prohibit direct transmission, the data controller shall explain those impediments to the data subjects, as his decision will otherwise be similar in its effect to a refusal to take action on a data subject’s request (Article 12(4)).

On a technical level, data controllers should explore and assess two different and complimentary paths for making portable data available to the data subjects or to other data controllers:

- a direct transmission of the overall dataset of portable data (or several extracts of parts of the global dataset);
- an automated tool that allows extraction of relevant data.

The second way may be preferred by data controllers in cases involving of complex and large data sets, as it allows for the extraction of any part of the data-set that is relevant for the data subject in the context of his or her request, may help minimising risk, and possibly allows for use of data synchronisation mechanisms\(^{30}\) (e.g. in the context of a regular communication between data controllers). It may be a better way to ensure compliance for the “new” data controller, and would constitute good practice in the reduction of privacy risks on the part of the initial data controller.

These two different and possibly complementary ways of providing relevant portable data could be implemented by making data available through various means such as, for example, secured messaging, an SFTP server, a secured WebAPI or WebPortal. Data subjects should be enabled to make use of a personal data store, personal information management system\(^{31}\) or other kinds of trusted third-parties, to hold and store the personal data and grant permission to data controllers to access and process the personal data as required.

- \textbf{What is the expected data format?}

The GDPR places requirements on data controllers to provide the personal data requested by the individual in a format, which supports re-use. Specifically, Article 20(1) of the GDPR states that the personal data must be provided “in a structured, commonly used and machine-

\(^{29}\) Through an authenticated communication with the necessary level of data encryption.

\(^{30}\) Synchronisation mechanism can help reaching the general obligations under Article 5 obligation of the GDPR, which provides that “personal data shall be (…) accurate and, where necessary, kept up to date”

\(^{31}\) On personal information management systems (PIMS), see, for example, EDPS Opinion 9/2016, available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-10-20_PIMS_opinion_EN.pdf
readable format”. Recital 68 provides a further clarification that this format should be interoperable, a term that is defined\(^{32}\) in the EU as:

> the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems.

The terms “structured”, “commonly used” and “machine-readable” are a set of minimal requirements that should facilitate the interoperability of the data format provided by the data controller. In that way, “structured, commonly used and machine readable” are specifications for the means, whereas interoperability is the desired outcome.

Recital 21 of Directive 2013/37/EU\(^{33,34}\) defines “machine readable” as:

> a file format structured so that software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal structure. Data encoded in files that are structured in a machine-readable format are machine-readable data. Machine-readable formats can be open or proprietary; they can be formal standards or not. Documents encoded in a file format that limits automatic processing, because the data cannot, or cannot easily, be extracted from them, should not be considered to be in a machine-readable format. Member States should where appropriate encourage the use of open, machine-readable formats.

Given the wide range of potential data types that could be processed by a data controller, the GDPR does not impose specific recommendations on the format of the personal data to be provided. The most appropriate format will differ across sectors and adequate formats may already exist, and should always be chosen to achieve the purpose of being interpretable and affording the data subject with a large degree of data portability. As such, formats that are subject to costly licensing constraints would not be considered an adequate approach.

Recital 68 clarifies that “The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible.” Thus, portability aims to produce interoperable systems, not compatible systems\(^{35}\).

Personal data are expected to be provided in formats that have a high level of abstraction from any internal or proprietary format. As such, data portability implies an additional layer of data processing by data controllers, in order to extract data from the platform and filter out personal data outside the scope of portability, such as inferred data or data related to security of systems. In this way, data controllers are encouraged to identify beforehand data which are within the scope of portability in their own systems. This additional data processing will be

---


\(^{33}\) Amending Directive 2003/98/EC on the re-use of public sector information.

\(^{34}\) The EU glossary (http://eur-lex.europa.eu/eli-register/glossary.html) provides further clarification on expectations related to the concepts used in this guideline, such as machine-readable, interoperability, open format, standard, metadata.

\(^{35}\) ISO/IEC 2382-01 defines interoperability as follows: “The capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units.”
considered as ancillary to the main data processing, since it is not performed to achieve a new purpose defined by the data controller.

Where no formats are in common use for a given industry or given context, data controllers should provide personal data using commonly used open formats (e.g. XML, JSON, CSV,…) along with useful metadata at the best possible level of granularity, while maintaining a high level of abstraction. As such, suitable metadata should be used in order to accurately describe the meaning of exchanged information. This metadata should be enough to make the function and reuse of the data possible but, of course, without revealing trade secrets. It is unlikely therefore that providing an individual with PDF versions of an email inbox would be sufficiently structured or descriptive to allow the inbox data to be easily re-used. Instead, the e-mail data should be provided in a format which preserves all the metadata, to allow the effective re-use of the data. As such, when selecting a data format in which to provide the personal data, the data controller should consider how this format would impact or hinder the individual’s right to re-use the data. In cases where a data controller is able to provide choices to the data subject regarding the preferred format of the personal data a clear explanation of the impact of the choice should be provided. However, processing additional metadata for the sole purpose that they might be needed or wanted to answer a data portability request poses no legitimate ground for such processing.

WP29 strongly encourages cooperation between industry stakeholders and trade associations to work together on a common set of interoperable standards and formats to deliver the requirements of the right to data portability. This challenge has also been addressed by the European Interoperability Framework (EIF) which has created an agreed approach to interoperability for organizations that wish to jointly deliver public services. Within its scope of applicability, the framework specifies a set of common elements such as vocabulary, concepts, principles, policies, guidelines, recommendations, standards, specifications and practices.

- How to deal with a large or complex personal data collection?

The GDPR does not explain how to address the challenge of responding where a large data collection, a complex data structure or other technical issues arise that might create difficulties for data controllers or data subjects.

However, in all cases, it is crucial that the individual is in a position to fully understand the definition, schema and structure of the personal data that could be provided by the data controller. For instance, data could first be provided in a summarised form using dashboards allowing the data subject to port subsets of the personal data rather than the entirety. The data controller should provide an overview “in a concise, transparent, intelligible and easily accessible form, using clear and plain language” (see Article 12(1)) of the GDPR in such a way that data subject should always have clear information of what data to download or transmit to another data controller in relation to a given purpose. For example, data subjects should be in a position to use software applications to easily identify, recognize and process specific data from it.

As referenced above, a practical way by which a data controller can answer requests for data portability may be by offering an appropriately secured and documented API. This may

enable individuals to make requests of the data controller for their personal data via their own or third-party software or grant permission for others to do so on their behalf (including another data controller) as specified in Article 20(2) of the GDPR. By granting access to data via an externally accessible API, it may also be possible to offer a more sophisticated access system that enables individuals to make subsequent requests for data, either as a full download or as a delta function containing only changes since the last download, without these additional requests being onerous on the data controller.

- **How can portable data be secured?**

In general, data controllers should guarantee the “appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures” according to Article 5(1)(f) of the GDPR.

However, the transmission of personal data to the data subject may also raise some security issues:

**How can data controllers ensure that personal data are securely delivered to the right person?**

As data portability aims to get personal data out of the information system of the data controller, the transmission may become a possible source of risk regarding those data (in particular of data breaches during the transmission). The data controller is responsible for taking all the security measures needed to ensure not only that personal data is securely transmitted (by the use of end-to-end or data encryption) to the right destination (by the use of strong authentication measures), but also continuing to protect the personal data that remains in their systems, as well as transparent procedures for dealing with possible data breaches.

As such, data controllers should assess the specific risks linked with data portability and take appropriate risks mitigation measures.

Such risk mitigation measures could include: if the data subject already needs to be authenticated, using additional authentication information, such as a shared secret, or another factor of authentication, such as a onetime password; suspending or freezing the transmission if there is suspicion that the account has been compromised; in cases of a direct transmission from a data controller to another data controller, authentication by mandate, such as token-based authentications, should be used.

Such security measures must not be obstructive in nature and must not prevent users from exercising their rights, e.g. by imposing additional costs.

**How to help users in securing the storage of their personal data in their own systems?**

By retrieving their personal data from an online service, there is always the risk that users may store them in less secured systems than the one provided by the service. The data subject requesting the data is responsible for identifying the right measures in order to secure personal data in his own system. However, he should be made aware of this in order to take steps to protect the information he has received. As an example of leading practice data controllers

---

37 In conformance to the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union
may also recommend appropriate format(s), encryption tools and other security measures to help the data subject in achieving this goal.

***

Done in Brussels, on 13 December 2016

For the Working Party,
The Chairwoman
Isabelle FALQUE-PIERROTIN

As last revised and adopted on 05 April 2017

For the Working Party
The Chairwoman
Isabelle FALQUE-PIERROTIN
THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE
PROCESSING OF PERSONAL DATA


having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT GUIDELINES:

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6938
Table of Contents

Introduction ........................................................................................................................................4

The meaning of transparency ..............................................................................................................6

Elements of transparency under the GDPR .....................................................................................6

“Concise, transparent, intelligible and easily accessible” .................................................................7

“Clear and plain language” .............................................................................................................8

Providing information to children and other vulnerable people ......................................................10

“In writing or by other means” .........................................................................................................11

“. . . the information may be provided orally” ..................................................................................12

“Free of charge” .............................................................................................................................13

Information to be provided to the data subject – Articles 13 & 14 .................................................13

Content ...........................................................................................................................................13

“Appropriate measures” ..................................................................................................................14

Timing for provision of information ...............................................................................................14

Changes to Article 13 and Article 14 information ..........................................................................16

Timing of notification of changes to Article 13 and Article 14 information .....................................17

Modalities - format of information provision ..................................................................................18

Layered approach in a digital environment and layered privacy statements/ notices ......................19

Layered approach in a non-digital environment .............................................................................20

“Push” and “pull” notices ..............................................................................................................20

Other types of “appropriate measures” ..........................................................................................21

Information on profiling and automated decision-making ..............................................................22

Other issues – risks, rules and safeguards .......................................................................................22

Information related to further processing .......................................................................................23

Visualisation tools ............................................................................................................................25

Icons ...............................................................................................................................................25

Certification mechanisms, seals and marks .....................................................................................26

Exercise of data subjects’ rights ......................................................................................................26

Exceptions to the obligation to provide information ......................................................................27

Article 13 exceptions ......................................................................................................................27

Article 14 exceptions ......................................................................................................................28
Proves impossible, disproportionate effort and serious impairment of objectives ..............................................28

“Proves impossible” ...........................................................................................................................................29

Impossibility of providing the source of the data .................................................................................................29

“Disproportionate effort” ......................................................................................................................................30

Serious impairment of objectives .........................................................................................................................31

Obtaining or disclosing is expressly laid down in law .............................................................................................32

Confidentiality by virtue of a secrecy obligation ....................................................................................................33

Restrictions on data subject rights ..........................................................................................................................33

Transparency and data breaches .............................................................................................................................34

Annex ........................................................................................................................................................................35
Introduction

1. These guidelines provide practical guidance and interpretative assistance from the Article 29 Working Party (WP29) on the new obligation of transparency concerning the processing of personal data under the General Data Protection Regulation1 (the "GDPR"). Transparency is an overarching obligation under the GDPR applying to three central areas: (1) the provision of information to data subjects related to fair processing; (2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and (3) how data controllers facilitate the exercise by data subjects of their rights2. Insofar as compliance with transparency is required in relation to data processing under Directive (EU) 2016/6803, these guidelines also apply to the interpretation of that principle.4 These guidelines are, like all WP29 guidelines, intended to be generally applicable and relevant to controllers irrespective of the sectoral, industry or regulatory specifications particular to any given data controller. As such, these guidelines cannot address the nuances and many variables which may arise in the context of the transparency obligations of a specific sector, industry or regulated area. However, these guidelines are intended to enable controllers to understand, at a high level, WP29’s interpretation of what the transparency obligations entail in practice and to indicate the approach which WP29 considers controllers should take to being transparent while embedding fairness and accountability into their transparency measures.

2. Transparency is a long established feature of the law of the EU5. It is about engendering trust in the processes which affect the citizen by enabling them to understand, and if necessary, challenge those processes. It is also an expression of the principle of fairness in relation to the

---

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

2 These guidelines set out general principles in relation to the exercise of data subjects’ rights rather than considering specific modalities for each of the individual data subject rights under the GDPR.

3 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

4 While transparency is not one of the principles relating to processing of personal data set out in Article 4 of Directive (EU) 2016/680, Recital 26 states that any processing of personal data must be “lawful, fair and transparent” in relation to the natural persons concerned.

5 Article 1 of the TEU refers to decisions being taken “as openly as possible and as close to the citizen as possible”; Article 11(2) states that “The institutions shall maintain an open, transparent and regular dialogue with representative associations and civil society”; and Article 15 of the TFEU refers amongst other things to citizens of the Union having a right of access to documents of Union institutions, bodies, offices and agencies and the requirements of those Union institutions, bodies, offices and agencies to ensure that their proceedings are transparent.
processing of personal data expressed in Article 8 of the Charter of Fundamental Rights of the European Union. Under the GDPR (Article 5(1)(a))\textsuperscript{6}, in addition to the requirements that data must be processed lawfully and fairly, transparency is now included as a fundamental aspect of these principles.\textsuperscript{7} Transparency is intrinsically linked to fairness and the new principle of accountability under the GDPR. It also follows from Article 5.2 that the controller must always be able to demonstrate that personal data are processed in a transparent manner in relation to the data subject.\textsuperscript{8} Connected to this, the accountability principle requires transparency of processing operations in order that data controllers are able to demonstrate compliance with their obligations under the GDPR.\textsuperscript{9}

3. In accordance with Recital 171 of the GDPR, where processing is already under way prior to 25 May 2018, a data controller should ensure that it is compliant with its transparency obligations as of 25 May 2018 (along with all other obligations under the GDPR). This means that prior to 25 May 2018, data controllers should revisit all information provided to data subjects on processing of their personal data (for example in privacy statements/notices etc.) to ensure that they adhere to the requirements in relation to transparency which are discussed in these guidelines. Where changes or additions are made to such information, controllers should make it clear to data subjects that these changes have been effected in order to comply with the GDPR. WP29 recommends that such changes or additions be actively brought to the attention of data subjects but at a minimum controllers should make this information publically available (e.g. on their website). However, if the changes or additions are material or substantive, then in line with paragraphs 29 to 32 below, such changes should be actively brought to the attention of the data subject.

4. Transparency, when adhered to by data controllers, empowers data subjects to hold data controllers and processors accountable and to exercise control over their personal data by, for example, providing or withdrawing informed consent and actioning their data subject rights\textsuperscript{10}. The concept of transparency in the GDPR is user-centric rather than legalistic and is realised by way of specific practical requirements on data controllers and processors in a number of articles. The practical (information) requirements are outlined in Articles 12 - 14 of the GDPR. However, the quality, accessibility and comprehensibility of the information is as important as the actual content of the transparency information, which must be provided to data subjects.

---

\textsuperscript{6}“Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject”.

\textsuperscript{7}In Directive 95/46/EC, transparency was only alluded to in Recital 38 by way of a requirement for processing of data to be fair, but not expressly referenced in the equivalent Article 6(1)(a).

\textsuperscript{8}Article 5.2 of the GDPR obliges a data controller to demonstrate transparency (together with the five other principles relating to data processing set out in Article 5.1) under the principle of accountability.

\textsuperscript{9}The obligation upon data controllers to implement technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with the GDPR is set out in Article 24.1.

\textsuperscript{10}See, for example, the Opinion of Advocate General Cruz Villalon (9 July 2015) in the Bara case (Case C-203/14) at paragraph 74: “the requirement to inform the data subjects about the processing of their personal data, which guarantees transparency of all processing, is all the more important since it affects the exercise by the data subjects of their right of access to the data being processed, referred to in Article 12 of Directive 95/46, and their right to object to the processing of those data, set out in Article 14 of that directive”. 

5. The transparency requirements in the GDPR apply irrespective of the legal basis for processing and throughout the life cycle of processing. This is clear from Article 12 which provides that transparency applies at the following stages of the data processing cycle:

- before or at the start of the data processing cycle, i.e. when the personal data is being collected either from the data subject or otherwise obtained;
- throughout the whole processing period, i.e. when communicating with data subjects about their rights; and
- at specific points while processing is ongoing, for example when data breaches occur or in the case of material changes to the processing.

The meaning of transparency

6. Transparency is not defined in the GDPR. Recital 39 of the GDPR is informative as to the meaning and effect of the principle of transparency in the context of data processing:

“It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed...”

Elements of transparency under the GDPR

7. The key articles in relation to transparency in the GDPR, as they apply to the rights of the data subject, are found in Chapter III (Rights of the Data Subject). Article 12 sets out the general rules which apply to: the provision of information to data subjects (under Articles 13 - 14); communications with data subjects concerning the exercise of their rights (under Articles 15 - 22); and communications in relation to data breaches (Article 34). In particular Article 12 requires that the information or communication in question must comply with the following rules:

- it must be concise, transparent, intelligible and easily accessible (Article 12.1);
- clear and plain language must be used (Article 12.1);
- the requirement for clear and plain language is of particular importance when providing information to children (Article 12.1);
- it must be in writing “or by other means, including where appropriate, by electronic means” (Article 12.1);
- where requested by the data subject it may be provided orally (Article 12.1); and
• it generally must be provided free of charge (Article 12.5).

"Concise, transparent, intelligible and easily accessible"

8. The requirement that the provision of information to, and communication with, data subjects is done in a “concise and transparent” manner means that data controllers should present the information/communication efficiently and succinctly in order to avoid information fatigue. This information should be clearly differentiated from other non-privacy related information such as contractual provisions or general terms of use. In an online context, the use of a layered privacy statement/notice will enable a data subject to navigate to the particular section of the privacy statement/notice which they want to immediately access rather than having to scroll through large amounts of text searching for particular issues.

9. The requirement that information is “intelligible” means that it should be understood by an average member of the intended audience. Intelligibility is closely linked to the requirement to use clear and plain language. An accountable data controller will have knowledge about the people they collect information about and it can use this knowledge to determine what that audience would likely understand. For example, a controller collecting the personal data of working professionals can assume its audience has a higher level of understanding than a controller that obtains the personal data of children. If controllers are uncertain about the level of intelligibility and transparency of the information and effectiveness of user interfaces/notices/policies etc., they can test these, for example, through mechanisms such as user panels, readability testing, formal and informal interactions and dialogue with industry groups, consumer advocacy groups and regulatory bodies, where appropriate, amongst other things.

10. A central consideration of the principle of transparency outlined in these provisions is that the data subject should be able to determine in advance what the scope and consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data has been used. This is also an important aspect of the principle of fairness under Article 5.1 of the GDPR and indeed is linked to Recital 39 which states that “[n]atural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data...” In particular, for complex, technical or unexpected data processing, WP29’s position is that, as well as providing the prescribed information under Articles 13 and 14 (dealt with later in these guidelines), controllers should also separately spell out in unambiguous language what the most important consequences of the processing will be: in other words, what kind of effect will the specific processing described in a privacy statement/notice actually have on a data subject? In accordance with the principle of accountability and in line with Recital 39, data controllers should assess whether there are particular risks for natural persons involved in this type of processing which should be brought to the attention of data subjects. This can help to provide an overview of the types of processing that could have the highest impact on the fundamental rights and freedoms of data subjects in relation to the protection of their personal data.
11. The "easily accessible" element means that the data subject should not have to seek out the information; it should be immediately apparent to them where and how this information can be accessed, for example by providing it directly to them, by linking them to it, by clearly signposting it or as an answer to a natural language question (for example in an online layered privacy statement/notice, in FAQs, by way of contextual pop-ups which activate when a data subject fills in an online form, or in an interactive digital context through a chatbot interface, etc. These mechanisms are further considered below, including at paragraphs 33 to 40).

Example

Every organisation that maintains a website should publish a privacy statement/notice on the website. A direct link to this privacy statement/notice should be clearly visible on each page of this website under a commonly used term (such as "Privacy", “Privacy Policy” or "Data Protection Notice"). Positioning or colour schemes that make a text or link less noticeable, or hard to find on a webpage, are not considered easily accessible.

For apps, the necessary information should also be made available from an online store prior to download. Once the app is installed, the information still needs to be easily accessible from within the app. One way to meet this requirement is to ensure that the information is never more than “two taps away” (e.g. by including a “Privacy”/ “Data Protection” option in the menu functionality of the app). Additionally, the privacy information in question should be specific to the particular app and should not merely be the generic privacy policy of the company that owns the app or makes it available to the public.

WP29 recommends as a best practice that at the point of collection of the personal data in an online context a link to the privacy statement/notice is provided or that this information is made available on the same page on which the personal data is collected.

"Clear and plain language"

12. With written information (and where written information is delivered orally, or by audio/audiovisual methods, including for vision-impaired data subjects), best practices for clear writing should be followed.11 A similar language requirement (for “plain, intelligible language”) has previously been used by the EU legislator12 and is also explicitly referred to in the context of consent in Recital 42 of the GDPR13. The requirement for clear and plain language means that information should be provided in as simple a manner as possible, avoiding complex sentence and language structures. The information should be concrete and definitive; it should not be phrased in abstract or ambivalent terms or leave room for different

---

13 Recital 42 states that a declaration of consent pre-formulated by a data controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms.
interpretations. In particular the purposes of, and legal basis for, processing the personal data should be clear.

**Poor Practice Examples**

The following phrases are not sufficiently clear as to the purposes of processing:

- "We may use your personal data to develop new services" (as it is unclear what the "services" are or how the data will help develop them);
- "We may use your personal data for research purposes" (as it is unclear what kind of "research" this refers to); and
- "We may use your personal data to offer personalised services" (as it is unclear what the "personalisation" entails).

**Good Practice Examples**

- "We will retain your shopping history and use details of the products you have previously purchased to make suggestions to you for other products which we believe you will also be interested in" (it is clear that what types of data will be processed, that the data subject will be subject to targeted advertisements for products and that their data will be used to enable this);
- "We will retain and evaluate information on your recent visits to our website and how you move around different sections of our website for analytics purposes to understand how people use our website so that we can make it more intuitive" (it is clear what type of data will be processed and the type of analysis which the controller is going to undertake); and
- "We will keep a record of the articles on our website that you have clicked on and use that information to target advertising on this website to you that is relevant to your interests, which we have identified based on articles you have read" (it is clear what the personalisation entails and how the interests attributed to the data subject have been identified).

13. Language qualifiers such as “may”, “might”, “some”, “often” and “possible” should also be avoided. Where data controllers opt to use indefinite language, they should be able, in accordance with the principle of accountability, to demonstrate why the use of such language could not be avoided and how it does not undermine the fairness of processing. Paragraphs and sentences should be well structured, utilising bullets and indents to signal hierarchical

---

14 The requirement for transparency exists entirely independently of the requirement upon data controllers to ensure that there is an appropriate legal basis for the processing under Article 6.
relationships. Writing should be in the active instead of the passive form and excess nouns should be avoided. The information provided to a data subject should not contain overly legalistic, technical or specialist language or terminology. Where the information is translated into one or more other languages, the data controller should ensure that all the translations are accurate and that the phraseology and syntax makes sense in the second language(s) so that the translated text does not have to be deciphered or re-interpreted. (A translation in one or more other languages should be provided where the controller targets data subjects speaking those languages.)

Providing information to children and other vulnerable people

14. Where a data controller is targeting children or is, or should be, aware that their goods/services are particularly utilised by children (including where the controller is relying on the consent of the child), it should ensure that the vocabulary, tone and style of the language used is appropriate to and resonates with children so that the child addressee of the information recognises that the message/information is being directed at them. A useful example of child-centred language used as an alternative to the original legal language can be found in the "UN Convention on the Rights of the Child in Child Friendly Language". 19

15. WP29’s position is that transparency is a free-standing right which applies as much to children as it does to adults. WP29 emphasises in particular that children do not lose their rights as data subjects to transparency simply because consent has been given/authorised by the holder of parental responsibility in a situation to which Article 8 of the GDPR applies. While such consent will, in many cases, be given or authorised on a once-off basis by the holder of parental responsibility, a child (like any other data subject) has an ongoing right to transparency throughout the continuum of their engagement with a data controller. This is consistent with Article 13 of the UN Convention on the Rights of the Child which states that a child has a right to freedom of expression which includes the right to seek, receive and impart information and ideas of all kinds. 20 It is important to point out that, while providing for consent to be given on behalf of a child when under a particular age, Article 8 does not provide for transparency measures to be directed at the holder of parental responsibility who

---

15 For example, where the controller operates a website in the language in question and/or offers specific country options and/or facilitates the payment for goods or services in the currency of a particular member state then these may be indicative of a data controller targeting data subjects of a particular member state.

16 The term “child” is not defined under the GDPR, however WP29 recognises that, in accordance with the UN Convention on the Rights of the Child, which all EU Member States have ratified, a child is a person under the age of 18 years.

17 i.e. children of 16 years or older (or, where in accordance with Article 8.1 of the GDPR Member State national law has set the age of consent at a specific age between 13 and 16 years for children to consent to an offer for the provision of information society services, children who meet that national age of consent).

18 Recital 38 states that “Children merit special protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data”. Recital 58 states that “Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand”.


20 Article 13 of the UN Convention on the Rights of the Child states that: “The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child’s choice.”

21 See footnote 17 above.
gives such consent. Therefore, data controllers have an obligation in accordance with the specific mentions of transparency measures addressed to children in Article 12.1 (supported by Recitals 38 and 58) to ensure that where they target children or are aware that their goods or services are particularly utilised by children of a literate age, that any information and communication should be conveyed in clear and plain language or in a medium that children can easily understand. For the avoidance of doubt however, WP29 recognises that with very young or pre-literate children, transparency measures may also be addressed to holders of parental responsibility given that such children will, in most cases, be unlikely to understand even the most basic written or non-written messages concerning transparency.

16. Equally, if a data controller is aware that their goods/services are availed of by (or targeted at) other vulnerable members of society, including people with disabilities or people who may have difficulties accessing information, the vulnerabilities of such data subjects should be taken into account by the data controller in its assessment of how to ensure that it complies with its transparency obligations in relation to such data subjects.\(^2\) This relates to the need for a data controller to assess its audience's likely level of understanding, as discussed above at paragraph 9.

"In writing or by other means"

17. Under Article 12.1, the default position for the provision of information to, or communications with, data subjects is that the information is in writing.\(^3\) (Article 12.7 also provides for information to be provided in combination with standardised icons and this issue is considered in the section on visualisation tools at paragraphs 49 to 53). However, the GDPR also allows for other, unspecified “means” including electronic means to be used. WP29’s position with regard to written electronic means is that where a data controller maintains (or operates, in part or in full, through) a website, WP29 recommends the use of layered privacy statements/ notices, which allow website visitors to navigate to particular aspects of the relevant privacy statement/ notice that are of most interest to them (see more on layered privacy statements/notices at paragraph 35 to 37).\(^4\) However, the entirety of the information addressed to data subjects should also be available to them in one single place or one complete document (whether in a digital or paper format) which can be easily accessed by a data subject should they wish to consult the entirety of the information addressed to them. Importantly, the use of a layered approach is not confined only to written electronic means for providing information to data subjects. As discussed at paragraphs 35 to 36 and 38 below, a layered approach to the provision of information to data subjects may also be utilised by employing a combination of methods to ensure transparency in relation to processing.

---

\(^2\) For example, the UN Convention on the Rights of Persons with Disabilities requires that appropriate forms of assistance and support are provided to persons with disabilities to ensure their access to information.

\(^3\) Article 12.1 refers to “language” and states that the information shall be provided in writing, or by other means, including, where appropriate, by electronic means.

\(^4\) The WP29’s recognition of the benefits of layered notices has already been noted in Opinion 10/2004 on More Harmonised Information Provisions and Opinion 02/2013 on apps on smart devices.
18. Of course, the use of digital layered privacy statements/ notices is not the only written electronic means that can be deployed by controllers. Other electronic means include “just-in-time” contextual pop-up notices, 3D touch or hover-over notices, and privacy dashboards. Non-written electronic means which may be used in addition to a layered privacy statement/ notice might include videos and smartphone or IoT voice alerts. Other means, which are not necessarily electronic, might include, for example, cartoons, infographics or flowcharts. Where transparency information is directed at children specifically, controllers should consider what types of measures may be particularly accessible to children (e.g. these might be comics/ cartoons, pictograms, animations, etc. amongst other measures).

19. It is critical that the method(s) chosen to provide the information is/are appropriate to the particular circumstances, i.e. the manner in which the data controller and data subject interact or the manner in which the data subject’s information is collected. For example, only providing the information in electronic written format, such as in an online privacy statement/ notice may not be appropriate/ workable where a device that captures personal data does not have a screen (e.g. IoT devices/ smart devices) to access the website/ display such written information. In such cases, appropriate alternative additional means should be considered, for example providing the privacy statement/ notice in hard copy instruction manuals or providing the URL website address (i.e. the specific page on the website) at which the online privacy statement/ notice can be found in the hard copy instructions or in the packaging. Audio (oral) delivery of the information could also be additionally provided if the screenless device has audio capabilities. WP29 has previously made recommendations around transparency and provision of information to data subjects in its Opinion on Recent Developments in the Internet of Things (such as the use of QR codes printed on internet of things objects, so that when scanned, the QR code will display the required transparency information). These recommendations remain applicable under the GDPR.

"..the information may be provided orally"

20. Article 12.1 specifically contemplates that information may be provided orally to a data subject on request, provided that their identity is proven by other means. In other words, the means employed should be more than reliance on a mere assertion by the individual that they are a specific named person and the means should enable the controller to verify a data subject’s identity with sufficient assurance. The requirement to verify the identity of the data subject before providing information orally only applies to information relating to the exercise by a specific data subject of their rights under Articles 15 to 22 and 34. This precondition to the provision of oral information cannot apply to the provision of general privacy information as outlined in Articles 13 and 14, since information required under Articles 13 and 14 must also be made accessible to future users/ customers (whose identity a data controller would not be in a position to verify). Hence, information to be provided under

---

25 These examples of electronic means are indicative only and data controllers may develop new innovative methods to comply with Article 12.

26 WP29 Opinion 8/2014 adopted on 16 September 2014
Articles 13 and 14 may be provided by oral means without the controller requiring a data subject’s identity to be proven.

21. The oral provision of information required under Articles 13 and 14 does not necessarily mean oral information provided on a person-to-person basis (i.e. in person or by telephone). Automated oral information may be provided in addition to written means. For example, this may apply in the context of persons who are visually impaired when interacting with information society service providers, or in the context of screenless smart devices, as referred to above at paragraph 19. Where a data controller has chosen to provide information to a data subject orally, or a data subject requests the provision of oral information or communications, WP29’s position is that the data controller should allow the data subject to re-listen to pre-recorded messages. This is imperative where the request for oral information relates to visually impaired data subjects or other data subjects who may have difficulty in accessing or understanding information in written format. The data controller should also ensure that it has a record of, and can demonstrate (for the purposes of complying with the accountability requirement): (i) the request for the information by oral means, (ii) the method by which the data subject’s identity was verified (where applicable – see above at paragraph 20) and (iii) the fact that information was provided to the data subject.

"Free of charge"

22. Under Article 12.5, data controllers cannot generally charge data subjects for the provision of information under Articles 13 and 14, or for communications and actions taken under Articles 15 - 22 (on the rights of data subjects) and Article 34 (communication of personal data breaches to data subjects). This aspect of transparency also means that any information provided under the transparency requirements cannot be made conditional upon financial transactions, for example the payment for, or purchase of, services or goods.

Information to be provided to the data subject – Articles 13 & 14

Content

23. The GDPR lists the categories of information that must be provided to a data subject in relation to the processing of their personal data where it is collected from the data subject (Article 13) or obtained from another source (Article 14). The table in the Annex to these

---

27 This states that “Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge.”

28 However, under Article 12.5 the controller may charge a reasonable fee where, for example, a request by a data subject in relation to the information under Article 13 and 14 or the rights under Articles 15 - 22 or Article 34 is excessive or manifestly unfounded. (Separately, in relation to the right of access under Article 15.3 a controller may charge a reasonable fee based on administrative costs for any further copy of the personal data which is requested by a data subject).

29 By way of illustration, if a data subject’s personal data is being collected in connection with a purchase, the information which is required to be provided under Article 13 should be provided prior to payment being made and at the point at which the information is being collected, rather than after the transaction has been concluded. Equally though, where free services are being provided to the data subject, the Article 13 information must be provided prior to, rather than after, sign-up given that Article 13.1 requires the provision of the information “at the time when the personal data are obtained”.

Page 13 of 40
guidelines summarises the categories of information that must be provided under Articles 13 and 14. It also considers the nature, scope and content of these requirements. For clarity, WP29’s position is that there is no difference between the status of the information to be provided under sub-article 1 and 2 of Articles 13 and 14 respectively. All of the information across these sub-articles is of equal importance and must be provided to the data subject.

"Appropriate measures"

As well as content, the form and manner in which the information required under Articles 13 and 14 should be provided to the data subject is also important. The notice containing such information is frequently referred to as a data protection notice, privacy notice, privacy policy, privacy statement or fair processing notice. The GDPR does not prescribe the format or modality by which such information should be provided to the data subject but does make it clear that it is the data controller’s responsibility to take “appropriate measures” in relation to the provision of the required information for transparency purposes. This means that the data controller should take into account all of the circumstances of the data collection and processing when deciding upon the appropriate modality and format of the information provision. In particular, appropriate measures will need to be assessed in light of the product/service user experience. This means taking account of the device used (if applicable), the nature of the user interfaces/interactions with the data controller (the user “journey”) and the limitations that those factors entail. As noted above at paragraph 17, WP29 recommends that where a data controller has an online presence, an online layered privacy statement/notice should be provided.

In order to help identify the most appropriate modality for providing the information, in advance of “going live”, data controllers may wish to trial different modalities by way of user testing (e.g. hall tests, or other standardised tests of readability or accessibility) to seek feedback on how accessible, understandable and easy to use the proposed measure is for users. (See also further comments above on other mechanisms for carrying out user testing at paragraph 9). Documenting this approach should also assist data controllers with their accountability obligations by demonstrating how the tool/approach chosen to convey the information is the most appropriate in the circumstances.

Timing for provision of information

Articles 13 and 14 set out information which must be provided to the data subject at the commencement phase of the processing cycle\(^{30}\). Article 13 applies to the scenario where the data is collected from the data subject. This includes personal data that:

\(^{30}\) Pursuant to the principles of fairness and purpose limitation, the organisation which collects the personal data from the data subject should always specify the purposes of the processing at the time of collection. If the purpose includes the creation of inferred personal data, the intended purpose of creating and further processing such inferred personal data, as well as the categories of the inferred data processed, must always be communicated to the data subject at the time of collection, or prior to the further processing for a new purpose in compliance with Article 13.3 or Article 14.4.
• a data subject consciously provides to a data controller (e.g. when completing an online form); or
• a data controller collects from a data subject by observation (e.g. using automated data capturing devices or data capturing software such as cameras, network equipment, Wi-Fi tracking, RFID or other types of sensors).

Article 14 applies in the scenario where the data have not been obtained from the data subject. This includes personal data which a data controller has obtained from sources such as:

• third party data controllers;
• publicly available sources;
• data brokers; or
• other data subjects.

27. As regards timing of the provision of this information, providing it in a timely manner is a vital element of the transparency obligation and the obligation to process data fairly. Where Article 13 applies, under Article 13.1 the information must be provided "at the time when personal data are obtained". In the case of indirectly obtained personal data under Article 14, the timeframes within which the required information must be provided to the data subject are set out in Article 14.3 (a) to (c) as follows:

• The general requirement is that the information must be provided within a "reasonable period" after obtaining the personal data and no later than one month, "having regard to the specific circumstances in which the personal data are processed" (Article 14.3(a)).

• The general one-month time limit in Article 14.3(a) may be further curtailed under Article 14.3(b),\(^{31}\) which provides for a situation where the data are being used for communication with the data subject. In such a case, the information must be provided at the latest at the time of the first communication with the data subject. If the first communication occurs prior to the one-month time limit after obtaining the personal data, then the information must be provided at the latest at the time of the first communication with the data subject notwithstanding that one month from the point of obtaining the data has not expired. If the first communication with a data subject occurs more than one month after obtaining the personal data then Article 14.3(a) continues to apply, so that the Article 14 information must be provided to the data subject at the latest within one month after it was obtained.

---

\(^{31}\) The use of the words "if the personal data are to be used for..." in Article 14.3(b) indicates a specification to the general position with regard to the maximum time limit set out in Article 14.3(a) but does not replace it.
The general one-month time limit in Article 14.3(a) can also be curtailed under Article 14.3(c)\textsuperscript{32} which provides for a situation where the data are being disclosed to another recipient (whether a third party or not)\textsuperscript{33}. In such a case, the information must be provided at the latest at the time of the first disclosure. In this scenario, if the disclosure occurs prior to the one-month time limit, then the information must be provided at the latest at the time of that first disclosure, notwithstanding that one month from the point of obtaining the data has not expired. Similar to the position with Article 14.3(b), if any disclosure of the personal data occurs more than one month after obtaining the personal data, then Article 14.3(a) again continues to apply, so that the Article 14 information must be provided to the data subject at the latest within one month after it was obtained.

Therefore, in any case, the maximum time limit within which Article 14 information must be provided to a data subject is one month. However, the principles of fairness and accountability under the GDPR require data controllers to always consider the reasonable expectations of data subjects, the effect that the processing may have on them and their ability to exercise their rights in relation to that processing, when deciding at what point to provide the Article 14 information. Accountability requires controllers to demonstrate the rationale for their decision and justify why the information was provided at the time it was. In practice, it may be difficult to meet these requirements when providing information at the 'last moment'. In this regard, Recital 39 stipulates, amongst other things, that data subjects should be "made aware of the risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing". Recital 60 also refers to the requirement that the data subject be informed of the existence of the processing operation and its purposes in the context of the principles of fair and transparent processing. For all of these reasons, WP29's position is that, wherever possible, data controllers should, in accordance with the principle of fairness, provide the information to data subjects well in advance of the stipulated time limits. Further comments on the appropriateness of the timeframe between notifying data subjects of the processing operations and such processing operations actually taking effect are set out in paragraphs 30 to 31 and 48.

Changes to Article 13 and Article 14 information

Being accountable as regards transparency applies not only at the point of collection of personal data but throughout the processing life cycle, irrespective of the information or communication being conveyed. This is the case, for example, when changing the contents of existing privacy statements/ notices. The controller should adhere to the same principles when communicating both the initial privacy statement/ notice and any subsequent substantive or material changes to this statement/ notice. Factors which controllers should consider in assessing what is a substantive or material change include the impact on data subjects (including their ability to exercise their rights), and how unexpected/ surprising the...
change would be to data subjects. Changes to a privacy statement/notice that should always be communicated to data subjects include inter alia: a change in processing purpose; a change to the identity of the controller; or a change as to how data subjects can exercise their rights in relation to the processing. Conversely, an example of changes to a privacy statement/notice which are not considered by WP29 to be substantive or material include corrections of misspellings, or stylistic/grammatical flaws. Since most existing customers or users will only glance over communications of changes to privacy statements/notifications, the controller should take all measures necessary to ensure that these changes are communicated in such a way that ensures that most recipients will actually notice them. This means, for example, that a notification of changes should always be communicated by way of an appropriate modality (e.g. email, hard copy letter, pop-up on a webpage or other modality which will effectively bring the changes to the attention of the data subject) specifically devoted to those changes (e.g. not together with direct marketing content), with such a communication meeting the Article 12 requirements of being concise, transparent, intelligible, easily accessible and using clear and plain language. References in the privacy statement/notice to the effect that the data subject should regularly check the privacy statement/notice for changes or updates are considered not only insufficient but also unfair in the context of Article 5.1(a). Further guidance in relation to the timing for notification of changes to data subjects is considered below at paragraph 30 to 31.

**Timing of notification of changes to Article 13 and Article 14 information**

30. The GDPR is silent on the timing requirements (and indeed the methods) that apply for notifications of changes to information that has previously been provided to a data subject under Article 13 or 14 (excluding an intended further purpose for processing, in which case information on that further purpose must be notified prior to the commencement of that further processing as per Articles 13.3 and 14.4 – see below at paragraph 31 and 32). However, as noted above in the context of the timing for the provision of Article 14 information, the data controller must again have regard to the fairness and accountability principles in terms of any reasonable expectations of the data subject, or the potential impact of those changes upon the data subject. If the change to the information is indicative of a fundamental change to the nature of the processing (e.g. enlargement of the categories of recipients or introduction of transfers to a third country) or a change which may not be fundamental in terms of the processing operation but which may be relevant to and impact upon the data subject, then that information should be provided to the data subject well in advance of the change actually taking effect and the method used to bring the changes to the data subject’s attention should be explicit and effective. This is to ensure the data subject does not “miss” the change and to allow the data subject a reasonable timeframe for them to (a) consider the nature and impact of the change and (b) exercise their rights under the GDPR in relation to the change (e.g. to withdraw consent or to object to the processing).

31. Data controllers should carefully consider the circumstances and context of each situation where an update to transparency information is required, including the potential impact of the changes upon the data subject and the modality used to communicate the changes, and be able to demonstrate how the timeframe between notification of the changes and the
change taking effect satisfies the principle of fairness to the data subject. Further, WP29’s position is that, consistent with the principle of fairness, when notifying such changes to data subjects, a data controller should also explain what will be the likely impact of those changes on data subjects. However, compliance with transparency requirements does not “whitewash” a situation where the changes to the processing are so significant that the processing becomes completely different in nature to what it was before. WP29 emphasises that all of the other rules in the GDPR, including those relating to incompatible further processing, continue to apply irrespective of compliance with the transparency obligations.

32. Additionally, even when transparency information (e.g. contained in a privacy statement/notice) does not materially change, it is likely that data subjects who have been using a service for a significant period of time will not recall the information provided to them at the outset under Articles 13 and/or 14. WP29 recommends that controllers facilitate data subjects to have continuing easy access to the information to re-acquaint themselves with the scope of the data processing. In accordance with the accountability principle, controllers should also consider whether, and at what intervals, it is appropriate for them to provide express reminders to data subjects as to the fact of the privacy statement/notice and where they can find it.

Modalities - format of information provision

33. Both Articles 13 and 14 refer to the obligation on the data controller to “provide the data subject with all of the following information...” The operative word here is “provide”. This means that the data controller must take active steps to furnish the information in question to the data subject or to actively direct the data subject to the location of it (e.g. by way of a direct link, use of a QR code, etc.). The data subject must not have to actively search for information covered by these articles amongst other information, such as terms and conditions of use of a website or app. The example at paragraph 11 illustrates this point. As noted above at paragraph 17, WP29 recommends that the entirety of the information addressed to data subjects should also be available to them in one single place or one complete document (e.g. whether in a digital form on a website or in paper format) which can be easily accessed should they wish to consult the entirety of the information.

34. There is an inherent tension in the GDPR between the requirements on the one hand to provide the comprehensive information to data subjects which is required under the GDPR, and on the other hand do so in a form that is concise, transparent, intelligible and easily accessible. As such, and bearing in mind the fundamental principles of accountability and fairness, controllers must undertake their own analysis of the nature, circumstances, scope and context of the processing of personal data which they carry out and decide, within the legal requirements of the GDPR and taking account of the recommendations in these Guidelines particularly at paragraph 36 below, how to prioritise information which must be provided to data subjects and what are the appropriate levels of detail and methods for conveying the information.
Layered approach in a digital environment and layered privacy statements/ notices

35. In the digital context, in light of the volume of information which is required to be provided to the data subject, a layered approach may be followed by data controllers where they opt to use a combination of methods to ensure transparency. WP29 recommends in particular that layered privacy statements/ notices should be used to link to the various categories of information which must be provided to the data subject, rather than displaying all such information in a single notice on the screen, in order to avoid information fatigue. Layered privacy statements/ notices can help resolve the tension between completeness and understanding, notably by allowing users to navigate directly to the section of the statement/ notice that they wish to read. It should be noted that layered privacy statements/ notices are not merely nested pages that require several clicks to get to the relevant information. The design and layout of the first layer of the privacy statement/ notice should be such that the data subject has a clear overview of the information available to them on the processing of their personal data and where/ how they can find that detailed information within the layers of the privacy statement/ notice. It is also important that the information contained within the different layers of a layered notice is consistent and that the layers do not provide conflicting information.

36. As regards the content of the first modality used by a controller to inform data subjects in a layered approach (in other words the primary way in which the controller first engages with a data subject), or the content of the first layer of a layered privacy statement/ notice, WP29 recommends that the first layer/ modality should include the details of the purposes of processing, the identity of controller and a description of the data subject’s rights. (Furthermore this information should be directly brought to the attention of a data subject at the time of collection of the personal data e.g. displayed as a data subject fills in an online form.) The importance of providing this information upfront arises in particular from Recital 39. While controllers must be able to demonstrate accountability as to what further information they decide to prioritise, WP29’s position is that, in line with the fairness principle, in addition to the information detailed above in this paragraph, the first layer/ modality should also contain information on the processing which has the most impact on the data subject and processing which could surprise them. Therefore, the data subject should be able to understand from information contained in the first layer/ modality what the consequences of the processing in question will be for the data subject (see also above at paragraph 10).

37. In a digital context, aside from providing an online layered privacy statement/ notice, data controllers may also choose to use additional transparency tools (see further examples considered below) which provide tailored information to the individual data subject which is specific to the position of the individual data subject concerned and the goods/ services which that data subject is availing of. It should be noted however that while WP29 recommends the

---

34 Recital 39 states, on the principle of transparency, that “That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed.”
use of online layered privacy statements/ notices, this recommendation does not exclude the development and use of other innovative methods of compliance with transparency requirements.

Layered approach in a non-digital environment

A layered approach to the provision of transparency information to data subjects can also be deployed in an offline/ non-digital context (i.e. a real-world environment such as person-to-person engagement or telephone communications) where multiple modalities may be deployed by data controllers to facilitate the provision of information. (See also paragraphs 33 to 37 and 39 to 40 in relation to different modalities for providing the information.) This approach should not be confused with the separate issue of layered privacy statements/ notices. Whatever the formats that are used in this layered approach, WP29 recommends that the first “layer” (in other words the primary way in which the controller first engages with the data subject) should generally convey the most important information (as referred to at paragraph 36 above), namely the details of the purposes of processing, the identity of controller and the existence of the rights of the data subject, together with information on the greatest impact of processing or processing which could surprise the data subject. For example, where the first point of contact with a data subject is by telephone, this information could be provided during the telephone call with the data subject and they could be provided with the balance of the information required under Article 13/14 by way of further, different means, such as by sending a copy of the privacy policy by email and/ or sending the data subject a link to the controller’s layered online privacy statement/ notice.

"Push" and "pull" notices

Another possible way of providing transparency information is through the use of “push” and “pull” notices. Push notices involve the provision of “just-in-time” transparency information notices while “pull” notices facilitate access to information by methods such as permission management, privacy dashboards and “learn more” tutorials. These allow for a more user-centric transparency experience for the data subject.

- A **privacy dashboard** is a single point from which data subjects can view ‘privacy information’ and manage their privacy preferences by allowing or preventing their data from being used in certain ways by the service in question. This is particularly useful when the same service is used by data subjects on a variety of different devices as it gives them access to and control over their personal data no matter how they use the service. Allowing data subjects to manually adjust their privacy settings via a privacy dashboard can also make it easier for a privacy statement/ notice to be personalised by reflecting only the types of processing occurring for that particular data subject. Incorporating a privacy dashboard into the existing architecture of a service (e.g. by using the same design and branding as the rest of the service) is preferable because it will ensure that access and use of it will be intuitive and may help to encourage users to engage with this information, in the same way that they would with other aspects of the service. This can be an effective way of
demonstrating that ‘privacy information’ is a necessary and integral part of a service rather than a lengthy list of legalese.

- A just-in-time notice is used to provide specific ‘privacy information’ in an ad hoc manner, as and when it is most relevant for the data subject to read. This method is useful for providing information at various points throughout the process of data collection; it helps to spread the provision of information into easily digestible chunks and reduces the reliance on a single privacy statement/notice containing information that is difficult to understand out of context. For example, if a data subject purchases a product online, brief explanatory information can be provided in pop-ups accompanying relevant fields of text. The information next to a field requesting the data subject’s telephone number could explain for example that this data is only being collected for the purposes of contact regarding the purchase and that it will only be disclosed to the delivery service.

Other types of "appropriate measures"

40. Given the very high level of internet access in the EU and the fact that data subjects can go online at any time, from multiple locations and different devices, as stated above, WP29’s position is that an "appropriate measure" for providing transparency information in the case of data controllers who maintain a digital/online presence, is to do so through an electronic privacy statement/notice. However, based on the circumstances of the data collection and processing, a data controller may need to additionally (or alternatively where the data controller does not have any digital/online presence) use other modalities and formats to provide the information. Other possible ways to convey the information to the data subject arising from the following different personal data environments may include the following modes applicable to the relevant environment which are listed below. As noted previously, a layered approach may be followed by controllers where they opt to use a combination of such methods while ensuring that the most important information (see paragraph 36 and 38) is always conveyed in the first modality used to communicate with the data subject.

a. Hard copy/paper environment, for example when entering into contracts by postal means: written explanations, leaflets, information in contractual documentation, cartoons, infographics or flowcharts;
b. Telephonic environment: oral explanations by a real person to allow interaction and questions to be answered or automated or pre-recorded information with options to hear further more detailed information;
c. Screenless smart technology/IoT environment such as Wi-Fi tracking analytics: icons, QR codes, voice alerts, written details incorporated into paper set-up instructions, videos incorporated into digital set-up instructions, written information on the smart device, messages sent by SMS or email, visible boards containing the information, public signage or public information campaigns;
d. Person to person environment, such as responding to opinion polls, registering in person for a service: oral explanations or written explanations provided in hard or soft copy format;
e. "Real-life" environment with CCTV/ drone recording: visible boards containing the information, public signage, public information campaigns or newspaper/ media notices.

**Information on profiling and automated decision-making**

41. Information on the existence of automated decision-making, including profiling, as referred to in Articles 22.1 and 22.4, together with meaningful information about the logic involved and the significant and envisaged consequences of the processing for the data subject, forms part of the obligatory information which must be provided to a data subject under Articles 13.2(f) and 14.2(g). WP29 has produced guidelines on automated individual decision-making and profiling which should be referred to for further guidance on how transparency should be given effect in the particular circumstances of profiling. It should be noted that, aside from the specific transparency requirements applicable to automated decision-making under Articles 13.2(f) and 14.2(g), the comments in these guidelines relating to the importance of informing data subjects as to the consequences of processing of their personal data, and the general principle that data subjects should not be taken by surprise by the processing of their personal data, equally apply to profiling generally (not just profiling which is captured by Article 22), as a type of processing.37

**Other issues – risks, rules and safeguards**

42. Recital 39 of the GDPR also refers to the provision of certain information which is not explicitly covered by Articles 13 and Article 14 (see recital text above at paragraph 28). The reference in this recital to making data subjects aware of the risks, rules and safeguards in relation to the processing of personal data is connected to a number of other issues. These include data protection impact assessments (DPIAs). As set out in the WP29 Guidelines on DPIAs, data controllers may consider publication of the DPIA (or part of it), as a way of fostering trust in the processing operations and demonstrating transparency and accountability, although such publication is not obligatory. Furthermore, adherence to a code of conduct (provided for under Article 40) may go towards demonstrating transparency, as codes of conduct may be drawn up for the purpose of specifying the application of the GDPR with regard to: fair and transparent processing; information provided to the public and to data subjects; and information provided to, and the protection of, children, amongst other issues.

43. Another relevant issue relating to transparency is data protection by design and by default (as required under Article 25). These principles require data controllers to build data

---

35 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251
36 This applies to decision-making based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects him or her.
37 Recital 60, which is relevant here, states that "Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling".
38 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.1
protection considerations into their processing operations and systems from the ground up, rather than taking account of data protection as a last-minute compliance issue. Recital 78 refers to data controllers implementing measures that meet the requirements of data protection by design and by default including measures consisting of transparency with regard to the functions and processing of personal data.

44. Separately, the issue of joint controllers is also related to making data subjects aware of the risks, rules and safeguards. Article 26.1 requires joint controllers to determine their respective responsibilities for complying with obligations under the GDPR in a transparent manner, in particular with regard to the exercise by data subjects of their rights and the duties to provide the information under Articles 13 and 14. Article 26.2 requires that the essence of the arrangement between the data controllers must be made available to the data subject. In other words, it must be completely clear to a data subject as to which data controller he or she can approach where they intend to exercise one or more of their rights under the GDPR. 39

Information related to further processing

45. Both Articles 13 and Article 14 contain a provision40 that requires a data controller to inform a data subject if it intends to further process their personal data for a purpose other than that for which it was collected/obtained. If so, “the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2”. These provisions specifically give effect to the principle in Article 5.1(b) that personal data shall be collected for specified, explicit and legitimate purposes, and further processing in a manner that is incompatible with these purposes is prohibited.41 The second part of Article 5.1(b) states that further processing for archiving purposes in the public interest, scientific or historical research purposes or for statistical purposes, shall, in accordance with Article 89.1, not be considered to be incompatible with the initial purposes. Where personal data are further processed for purposes that are compatible with the original purposes (Article 6.4 informs this issue42), Articles 13.3 and 14.4 apply. The requirements in these articles to inform a data subject about further processing promotes the position in the GDPR that a data subject should reasonably expect that at the time and in the context of the collection of personal data that processing

39 Under Article 26.3, irrespective of the terms of the arrangement between joint data controllers under Article 26.1, a data subject may exercise his or her rights under the GDPR in respect of and against each of the joint data controllers.
40 At Articles 13.3 and 14.4, which are expressed in identical terms, apart from the word “collected”, which is used in Article 13, and which is replaced with the word “obtained” in Article 14.
41 See, for example on this principle, Recitals 47, 50, 61, 156, 158; Articles 6.4 and 89
42 Article 6.4 sets out, in non-exhaustive fashion, the factors which are to be taken into account in ascertaining whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, namely: the link between the purposes; the context in which the personal data have been collected; the nature of the personal data (in particular whether special categories of personal data or personal data relating to criminal offences and convictions are included); the possible consequences of the intended further processing for data subjects; and the existence of appropriate safeguards.
for a particular purpose may take place.\textsuperscript{43} In other words, a data subject should not be taken by surprise at the purpose of processing of their personal data.

46. Articles 13.3 and 14.4, insofar as they refer to the provision of "any relevant further information as referred to in paragraph 2", may be interpreted at first glance as leaving some element of appreciation to the data controller as to the extent of and the particular categories of information from the relevant sub-paragraph 2 (i.e. Article 13.2 or 14.2 as applicable) that should be provided to the data subject. (Recital 61 refers to this as "other necessary information"). However the default position is that all such information set out in that sub-article should be provided to the data subject unless one or more categories of the information does not exist or is not applicable.

47. WP29 recommends that, in order to be transparent, fair and accountable, controllers should consider making information available to data subjects in their privacy statement/notice on the compatibility analysis carried out under Article 6.4 \textsuperscript{44} where a legal basis other than consent or national/EU law is relied on for the new processing purpose. (In other words, an explanation as to how the processing for the other purpose(s) is compatible with the original purpose). This is to allow data subjects the opportunity to consider the compatibility of the further processing and the safeguards provided and to decide whether to exercise their rights e.g. the right to restriction of processing or the right to object to processing, amongst others.\textsuperscript{45} Where controllers choose not to include such information in a privacy notice/statement, WP29 recommends that they make it clear to data subjects that they can obtain the information on request.

48. Connected to the exercise of data subject rights is the issue of timing. As emphasised above, the provision of information in a timely manner is a vital element of the transparency requirements under Articles 13 and 14 and is inherently linked to the concept of fair processing. Information in relation to further processing must be provided “prior to that further processing”. WP29’s position is that a reasonable period should occur between the notification and the processing commencing rather than an immediate start to the processing upon notification being received by the data subject. This gives data subjects the practical benefits of the principle of transparency, allowing them a meaningful opportunity to consider (and potentially exercise their rights in relation to) the further processing. What is a reasonable period will depend on the particular circumstances. The principle of fairness requires that the more intrusive (or less expected) the further processing, the longer the period should be. Equally, the principle of accountability requires that data controllers be able to demonstrate how the determinations they have made as regards the timing for the provision of this information are justified in the circumstances and how the timing overall is fair to data subjects. (See also the previous comments in relation to ascertaining reasonable timeframes above at paragraphs 30 to 32.)

\textsuperscript{43} Recitals 47 and 50
\textsuperscript{44} Also referenced in Recital 50
\textsuperscript{45} As referenced in Recital 63, this will enable a data subject to exercise the right of access in order to be aware of and to verify the lawfulness of the processing.
Visualisation tools

49. Importantly, the principle of transparency in the GDPR is not limited to being effected simply through language communications (whether written or oral). The GDPR provides for visualisation tools (referencing in particular, icons, certification mechanisms, and data protection seals and marks) where appropriate. Recital 58\(^6\) indicates that the accessibility of information addressed to the public or to data subjects is especially important in the online environment.\(^7\)

Icons

50. Recital 60 makes provision for information to be provided to a data subject “in combination” with standardised icons, thus allowing for a multi-layered approach. However, the use of icons should not simply replace information necessary for the exercise of a data subject’s rights nor should they be used as a substitute to compliance with the data controller’s obligations under Articles 13 and 14. Article 12.7 provides for the use of such icons stating that:

"The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where icons are presented electronically they shall be machine-readable”.

51. As Article 12.7 states that "Where the icons are presented electronically, they shall be machine-readable", this suggests that there may be situations where icons are not presented electronically,\(^8\) for example icons on physical paperwork, IoT devices or IoT device packaging, notices in public places about Wi-Fi tracking, QR codes and CCTV notices.

52. Clearly, the purpose of using icons is to enhance transparency for data subjects by potentially reducing the need for vast amounts of written information to be presented to a data subject. However, the utility of icons to effectively convey information required under Articles 13 and 14 to data subjects is dependent upon the standardisation of symbols/images to be

---

\(^6\) "Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising."

\(^7\) In this context, controllers should take into account visually impaired data subjects (e.g. red-green colour blindness).

\(^8\) There is no definition of “machine-readable” in the GDPR but Recital 21 of Directive 2013/37/EU\(^17\) defines “machine-readable” as:

>a file format structured so that software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal structure. Data encoded in files that are structured in a machine-readable format are machine-readable data. Machine-readable formats can be open or proprietary; they can be formal standards or not. Documents encoded in a file format that limits automatic processing, because the data cannot, or cannot easily, be extracted from them, should not be considered to be in a machine-readable format. Member States should where appropriate encourage the use of open, machine-readable formats.”
universally used and recognised across the EU as shorthand for that information. In this regard, the GDPR assigns responsibility for the development of a code of icons to the Commission but ultimately the European Data Protection Board may, either at the request of the Commission or of its own accord, provide the Commission with an opinion on such icons.⁴⁹ WP29 recognises that, in line with Recital 166, the development of a code of icons should be centred upon an evidence-based approach and in advance of any such standardisation it will be necessary for extensive research to be conducted in conjunction with industry and the wider public as to the efficacy of icons in this context.

_Certification mechanisms, seals and marks_

53. Aside from the use of standardised icons, the GDPR (Article 42) also provides for the use of data protection certification mechanisms, data protection seals and marks for the purpose of demonstrating compliance with the GDPR of processing operations by data controllers and processors and enhancing transparency for data subjects.⁵⁰ WP29 will be issuing guidelines on certification mechanisms in due course.

_Exercise of data subjects’ rights_

54. Transparency places a triple obligation upon data controllers insofar as the rights of data subjects under the GDPR are concerned, as they must:⁵¹

- provide information to data subjects on their rights (as required under Articles 13.2(b) and 14.2(c));
- comply with the principle of transparency (i.e. relating to the quality of the communications as set out in Article 12.1) when communicating with data subjects in relation to their rights under Articles 15 to 22 and 34; and
- facilitate the exercise of data subjects’ rights under Articles 15 to 22.

55. The GDPR requirements in relation to the exercise of these rights and the nature of the information required are designed to meaningfully position data subjects so that they can vindicate their rights and hold data controllers accountable for the processing of their personal data. Recital 59 emphasises that “modalities should be provided for facilitating the exercise of the data subject’s rights” and that the data controller should “also provide means

---

⁴⁹ Article 12.8 provides that the Commission is empowered to adopt delegated acts under Article 92 for the purpose of determining the information to be presented by the icons and the information for providing standardised icons. Recital 166 (which deals with delegated acts of the Commission in general) is instructive, providing that the Commission must carry out appropriate consultations during its preparatory work, including at expert level. However, the European Data Protection Board (EDPB) also has an important consultative role to play in relation to the standardisation of icons as Article 70.1(r) states that the EDPB shall on its own initiative or, where relevant, at the request of the Commission, provide the Commission with an opinion on icons.

⁵⁰ See the reference in Recital 100

⁵¹ Under the Transparency and Modalities section of the GDPR on Data Subject Rights (Section 1, Chapter III, namely Article 12)

⁵² Access, rectification, erasure, restriction on processing, object to processing, portability
for requests to be made electronically, especially where personal data are processed by electronic means”. The modality provided by a data controller for data subjects to exercise their rights should be appropriate to the context and the nature of the relationship and interactions between the controller and a data subject. To this end, a data controller may wish to provide one or more different modalities for the exercise of rights that are reflective of the different ways in which data subjects interact with that data controller.

Example

A health service provider uses an electronic form on its website, and paper forms in the receptions of its health clinics, to facilitate the submission of access requests for personal data both online and in person. While it provides these modalities, the health service still accepts access requests submitted in other ways (such as by letter and by email) and provides a dedicated point of contact (which can be accessed by email and by telephone) to help data subjects with the exercise of their rights.

Exceptions to the obligation to provide information

Article 13 exceptions

56. The only exception to a data controller’s Article 13 obligations where it has collected personal data directly from a data subject occurs “where and insofar as, the data subject already has the information”.53 The principle of accountability requires that data controllers demonstrate (and document) what information the data subject already has, how and when they received it and that no changes have since occurred to that information that would render it out of date. Further, the use of the phrase “insofar as” in Article 13.4 makes it clear that even if the data subject has previously been provided with certain categories from the inventory of information set out in Article 13, there is still an obligation on the data controller to supplement that information in order to ensure that the data subject now has a complete set of the information listed in Articles 13.1 and 13.2. The following is a best practice example concerning the limited manner in which the Article 13.4 exception should be construed.

Example

An individual signs up to an online email service and receives all of the required Article 13.1 and 13.2 information at the point of sign-up. Six months later the data subject activates a connected instant message functionality through the email service provider and provides their mobile telephone number to do so. The service provider gives the data subject certain Article 13.1 and 13.2 information about the processing of the telephone number (e.g. purposes and legal basis for processing, recipients, retention period) but does not provide other information that the individual already

---

53 Article 13.4
has from 6 months ago and which has not since changed (e.g. the identity and contact
details of the controller and the data protection officer, information on data subject
rights and the right to complain to the relevant supervisory authority). As a matter of
best practice however, the complete suite of information should be provided to the
data subject again but the data subject also should be able to easily tell what
information amongst it is new. The new processing for the purposes of the instant
messaging service may affect the data subject in a way which would prompt them to
seek to exercise a right they may have forgotten about, having been informed six
months prior. Providing all the information again helps to ensure the data subject
remains well informed about how their data is being used and their rights.

\[57.\]

\textbf{Article 14 exceptions}

Article 14 carves out a much broader set of exceptions to the information obligation on a data
controller where personal data has not been obtained from the data subject. These
exceptions should, as a general rule, be interpreted and applied narrowly. In addition to the
circumstances where the data subject already has the information in question (Article
14.5(a)), Article 14.5 also allows for the following exceptions:

- The provision of such information is impossible or would involve a disproportionate
effort, in particular for processing for archiving purposes in the public interest,
scientific or historical research purposes or statistical purposes, or where it would
make the achievement of the objectives of the processing impossible or seriously
impair them;
- The data controller is subject to a national law or EU law requirement to obtain or
disclose the personal data and that
the law provides appropriate protections for
the data subject’s legitimate interests ; or
- An obligation of professional secrecy (including a statutory obligation of secrecy)
which is regulated by national or EU law means the personal data must remain
confidential.

\[58.\]

\textbf{Proves impossible, disproportionate effort and serious impairment of objectives}

Article 14.5(b) allows for 3 separate situations where the obligation to provide the
information set out in Articles 14.1, 14.2 and 14.4 is lifted:

(i) Where it proves impossible (in particular for archiving, scientific/ historical research
or statistical purposes);
(ii) Where it would involve a disproportionate effort (in particular for archiving, scientific/
historical research or statistical purposes); or
(iii) Where providing the information required under Article 14.1 would make the
achievement of the objectives of the processing impossible or seriously impair them.
"Proves impossible"

59. The situation where it “proves impossible” under Article 14.5(b) to provide the information is an all or nothing situation because something is either impossible or it is not; there are no degrees of impossibility. Thus if a data controller seeks to rely on this exemption it must demonstrate the factors that actually prevent it from providing the information in question to data subjects. If, after a certain period of time, the factors that caused the “impossibility” no longer exist and it becomes possible to provide the information to data subjects then the data controller should immediately do so. In practice, there will be very few situations in which a data controller can demonstrate that it is actually impossible to provide the information to data subjects. The following example demonstrates this.

**Example**

A data subject registers for a post-paid online subscription service. After registration, the data controller collects credit data from a credit-reporting agency on the data subject in order to decide whether to provide the service. The controller’s protocol is to inform data subjects of the collection of this credit data within three days of collection, pursuant to Article 14.3(a). However, the data subject’s address and phone number is not registered in public registries (the data subject is in fact living abroad). The data subject did not leave an email address when registering for the service or the email address is invalid. The controller finds that it has no means to directly contact the data subject. In this case, however, the controller may give information about collection of credit reporting data on its website, prior to registration. In this case, it would not be impossible to provide information pursuant to Article 14.

**Impossibility of providing the source of the data**

60. Recital 61 states that “where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided”. The lifting of the requirement to provide data subjects with information on the source of their personal data applies only where this is not possible because different pieces of personal data relating to the same data subject cannot be attributed to a particular source. For example, the mere fact that a database comprising the personal data of multiple data subjects has been compiled by a data controller using more than one source is not enough to lift this requirement if it is possible (although time consuming or burdensome) to identify the source from which the personal data of individual data subjects derived. Given the requirements of data protection by design and by default, transparency mechanisms should be built into processing systems from the ground up so that all sources of personal data received into an organisation can be tracked and traced back to their source at any point in the data processing life cycle (see paragraph 43 above).

54 Article 25
"Disproportionate effort"

61. Under Article 14.5(b), as with the “proves impossible” situation, “disproportionate effort” may also apply, in particular, for processing “for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the safeguards referred to in Article 89(1)”. Recital 62 also references these objectives as cases where the provision of information to the data subject would involve a disproportionate effort and states that in this regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration. Given the emphasis in Recital 62 and Article 14.5(b) on archiving, research and statistical purposes with regard to the application of this exemption, WP29’s position is that this exception should not be routinely relied upon by data controllers who are not processing personal data for the purposes of archiving in the public interest, for scientific or historical research purposes or statistical purposes. WP29 emphasises the fact that where these are the purposes pursued, the conditions set out in Article 89.1 must still be complied with and the provision of the information must constitute a disproportionate effort.

62. In determining what may constitute either impossibility or disproportionate effort under Article 14.5(b), it is relevant that there are no comparable exemptions under Article 13 (where personal data is collected from a data subject). The only difference between an Article 13 and an Article 14 situation is that in the latter, the personal data is not collected from the data subject. It therefore follows that impossibility or disproportionate effort typically arises by virtue of circumstances which do not apply if the personal data is collected from the data subject. In other words, the impossibility or disproportionate effort must be directly connected to the fact that the personal data was obtained other than from the data subject.

Example

A large metropolitan hospital requires all patients for day procedures, longer-term admissions and appointments to fill in a Patient Information Form which seeks the details of two next-of-kin (data subjects). Given the very large volume of patients passing through the hospital on a daily basis, it would involve disproportionate effort on the part of the hospital to provide all persons who have been listed as next-of-kin on forms filled in by patients each day with the information required under Article 14.

63. The factors referred to above in Recital 62 (number of data subjects, the age of the data and any appropriate safeguards adopted) may be indicative of the types of issues that contribute to a data controller having to use disproportionate effort to notify a data subject of the relevant Article 14 information.

Example

Historical researchers seeking to trace lineage based on surnames indirectly obtain a large dataset relating to 20,000 data subjects. However, the dataset was collected 50
years ago, has not been updated since, and does not contain any contact details. Given the size of the database and more particularly, the age of the data, it would involve disproportionate effort for the researchers to try to trace the data subjects individually in order to provide them with Article 14 information.

64. Where a data controller seeks to rely on the exception in Article 14.5(b) on the basis that provision of the information would involve a disproportionate effort, it should carry out a balancing exercise to assess the effort involved for the data controller to provide the information to the data subject against the impact and effects on the data subject if he or she was not provided with the information. This assessment should be documented by the data controller in accordance with its accountability obligations. In such a case, Article 14.5(b) specifies that the controller must take appropriate measures to protect the data subject’s rights, freedoms and legitimate interests. This applies equally where a controller determines that the provision of the information proves impossible, or would likely render impossible or seriously impair the achievement of the objectives of the processing. One appropriate measure, as specified in Article 14.5(b), that controllers must always take is to make the information publicly available. A controller can do this in a number of ways, for instance by putting the information on its website, or by proactively advertising the information in a newspaper or on posters on its premises. Other appropriate measures, in addition to making the information publicly available, will depend on the circumstances of the processing, but may include: undertaking a data protection impact assessment; applying pseudonymisation techniques to the data; minimising the data collected and the storage period; and implementing technical and organisational measures to ensure a high level of security. Furthermore, there may be situations where a data controller is processing personal data which does not require the identification of a data subject (for example with pseudonymised data). In such cases, Article 11.1 may also be relevant as it states that a data controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purposes of complying with the GDPR.

**Serious impairment of objectives**

65. The final situation covered by Article 14.5(b) is where a data controller’s provision of the information to a data subject under Article 14.1 is likely to make impossible or seriously impair the achievement of the processing objectives. To rely on this exception, data controllers must demonstrate that the provision of the information set out in Article 14.1 alone would nullify the objectives of the processing. Notably, reliance on this aspect of Article 14.5(b) presupposes that the data processing satisfies all of the principles set out in Article 5 and that most importantly, in all of the circumstances, the processing of the personal data is fair and that it has a legal basis.

**Example**

Bank A is subject to a mandatory requirement under anti-money laundering legislation to report suspicious activity relating to accounts held with it to the relevant financial law enforcement authority. Bank A receives information from Bank B (in
another Member State) that an account holder has instructed it to transfer money to another account held with Bank A which appears suspicious. Bank A passes this data concerning its account holder and the suspicious activities to the relevant financial law enforcement authority. The anti-money laundering legislation in question makes it a criminal offence for a reporting bank to “tip off” the account holder that they may be subject to regulatory investigations. In this situation, Article 14.5(b) applies because providing the data subject (the account holder with Bank A) with Article 14 information on the processing of account holder’s personal data received from Bank B would seriously impair the objectives of the legislation, which includes the prevention of “tip-offs”. However, general information should be provided to all account holders with Bank A when an account is opened that their personal data may be processed for anti-money laundering purposes.

Obtaining or disclosing is expressly laid down in law

66. Article 14.5(c) allows for a lifting of the information requirements in Articles 14.1, 14.2 and 14.4 insofar as the obtaining or disclosure of personal data "is expressly laid down by Union or Member State law to which the controller is subject". This exemption is conditional upon the law in question providing "appropriate measures to protect the data subject's legitimate interests". Such a law must directly address the data controller and the obtaining or disclosure in question should be mandatory upon the data controller. Accordingly, the data controller must be able to demonstrate how the law in question applies to them and requires them to either obtain or disclose the personal data in question. While it is for Union or Member State law to frame the law such that it provides "appropriate measures to protect the data subject’s legitimate interests", the data controller should ensure (and be able to demonstrate) that its obtaining or disclosure of personal data complies with those measures. Furthermore, the data controller should make it clear to data subjects that it obtains or discloses personal data in accordance with the law in question, unless there is a legal prohibition preventing the data controller from doing so. This is in line with Recital 41 of the GDPR, which states that a legal basis or legislative measure should be clear and precise, and its application should be foreseeable to persons subject to it, in accordance with the case law of the Court of Justice of the EU and the European Court of Human Rights. However, Article 14.5(c) will not apply where the data controller is under an obligation to obtain data directly from a data subject, in which case Article 13 will apply. In that case, the only exemption under the GDPR exempting the controller from providing the data subject with information on the processing will be that under Article 13.4 (i.e. where and insofar as the data subject already has the information). However, as referred to below at paragraph 68, at a national level, Member States may also legislate, in accordance with Article 23, for further specific restrictions to the right to transparency under Article 12 and to information under Articles 13 and 14.

Example

A tax authority is subject to a mandatory requirement under national law to obtain the details of employees' salaries from their employers. The personal data is not obtained
from the data subjects and therefore the tax authority is subject to the requirements of Article 14. As the obtaining of the personal data by the tax authority from employers is expressly laid down by law, the information requirements in Article 14 do not apply to the tax authority in this instance.

Confidentiality by virtue of a secrecy obligation

67. Article 14.5(d) provides for an exemption to the information requirement upon data controllers where the personal data "must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy". Where a data controller seeks to rely on this exemption, it must be able to demonstrate that it has appropriately identified such an exemption and to show how the professional secrecy obligation directly addresses the data controller such that it prohibits the data controller from providing all of the information set out in Articles 14.1, 14.2 and 14.4 to the data subject.

Example

A medical practitioner (data controller) is under a professional obligation of secrecy in relation to his patients' medical information. A patient (in respect of whom the obligation of professional secrecy applies) provides the medical practitioner with information about her health relating to a genetic condition, which a number of her close relatives also have. The patient also provides the medical practitioner with certain personal data of her relatives (data subjects) who have the same condition. The medical practitioner is not required to provide those relatives with Article 14 information as the exemption in Article 14.5(d) applies. If the medical practitioner were to provide the Article 14 information to the relatives, the obligation of professional secrecy, which he owes to his patient, would be violated.

Restrictions on data subject rights

68. Article 23 provides for Member States (or the EU) to legislate for further restrictions on the scope of the data subject rights in relation to transparency and the substantive data subject rights\(^55\) where such measures respect the essence of the fundamental rights and freedoms and are necessary and proportionate to safeguard one or more of the ten objectives set out in Article 23.1(a) to (j). Where such national measures lessen either the specific data subject rights or the general transparency obligations, which would otherwise apply to data controllers under the GDPR, the data controller should be able to demonstrate how the national provision applies to them. As set out in Article 23.2(h), the legislative measure must contain a provision as to the right of the data subject to be informed about a restriction on

---

\(^{55}\) As set out in Articles 12 to 22 and 34, and in Article 5 insofar as its provisions correspond to the rights and obligations provided for in Articles 12 to 22.
their rights, unless so informing them may be prejudicial to the purpose of the restriction. Consistent with this, and in line with principle of fairness, the data controller should also inform data subjects that they are relying on (or will rely on, in the event of a particular data subject right being exercised) such a national legislative restriction to the exercise of data subject rights, or to the transparency obligation, unless doing so would be prejudicial to the purpose of the legislative restriction. As such, transparency requires data controllers to provide adequate upfront information to data subjects about their rights and any particular caveats to those rights which the controller may seek to rely on, so that the data subject is not taken by surprise at a purported restriction of a particular right when they later attempt to exercise it against the controller. In relation to pseudonymisation and data minimisation, and insofar as data controllers may purport to rely on Article 11 of the GDPR, WP29 has previously confirmed in Opinion 3/201756 that Article 11 of the GDPR should be interpreted as a way of enforcing genuine data minimisation without hindering the exercise of data subject rights, and that the exercise of data subject rights must be made possible with the help of additional information provided by the data subject.

69. Additionally, Article 85 requires Member States, by law, to reconcile data protection with the right to freedom of expression and information. This requires, amongst other things, that Member States provide for appropriate exemptions or derogations from certain provisions of the GDPR (including from the transparency requirements under Articles 12 - 14) for processing carried out for journalistic, academic, artistic or literary expression purposes, if they are necessary to reconcile the two rights.

**Transparency and data breaches**

70. WP29 has produced separate Guidelines on Data Breaches57 but for the purposes of these guidelines, a data controller’s obligations in relation to communication of data breaches to a data subject must take full account of the transparency requirements set out in Article 12.58 The communication of a data breach must satisfy the same requirements, detailed above (in particular for the use of clear and plain language), that apply to any other communication with a data subject in relation to their rights or in connection with conveying information under Articles 13 and 14.

---

56 Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS) – see paragraph 4.2
57 Guidelines on Personal data breach notification under Regulation 2016/679, WP 250
58 This is made clear by Article 12.1 which specifically refers to “…any communication under Articles 15 to 22 and 34 relating to processing to the data subject...” [emphasis added].
### Annex
Information that must be provided to a data subject under Article 13 or Article 14

<table>
<thead>
<tr>
<th>Required Information Type</th>
<th>Relevant article (if personal data collected directly from data subject)</th>
<th>Relevant article (if personal data not obtained from the data subject)</th>
<th>WP29 comments on information requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>The identity and contact details of the controller and, where applicable, their representative&lt;sup&gt;59&lt;/sup&gt;</td>
<td>Article 13.1(a)</td>
<td>Article 14.1(a)</td>
<td>This information should allow for easy identification of the controller and preferably allow for different forms of communications with the data controller (e.g. phone number, email, postal address, etc.)</td>
</tr>
<tr>
<td>Contact details for the data protection officer, where applicable</td>
<td>Article 13.1(b)</td>
<td>Article 14.1(b)</td>
<td>See WP29 Guidelines on Data Protection Officers&lt;sup&gt;60&lt;/sup&gt;</td>
</tr>
<tr>
<td>The purposes and legal basis for the processing</td>
<td>Article 13.1(c)</td>
<td>Article 14.1(c)</td>
<td>In addition to setting out the purposes of the processing for which the personal data is intended, the relevant legal basis relied upon under Article 6 must be specified. In the case of special categories of personal data, the relevant provision of Article 9 (and where relevant, the applicable Union or Member State law under which the data is processed) should be specified. Where, pursuant to Article 10, personal data relating to criminal convictions and offences or related security</td>
</tr>
</tbody>
</table>

---

<sup>59</sup> As defined by Article 4.17 of the GDPR (and referenced in Recital 80), “representative” means a natural or legal person established in the EU who is designated by the controller or processor in writing under Article 27 and represents the controller or processor with regard to their respective obligations under the GDPR. This obligation applies where, in accordance with Article 3.2, the controller or processor is not established in the EU but processes the personal data of data subjects who are in the EU, and the processing relates to the offer of goods or services to, or monitoring of the behaviour of, data subjects in the EU.

<sup>60</sup> Guidelines on Data Protection Officers, WP243 rev.01, last revised and adopted on 5 April 2017
| Measures based on Article 6.1 is processed, where applicable the relevant Union or Member State law under which the processing is carried out should be specified. |
|---|---|---|
| Where legitimate interests (Article 6.1(f)) is the legal basis for the processing, the legitimate interests pursued by the data controller or a third party | Article 13.1(d) | Article 14.2(b) | The specific interest in question must be identified for the benefit of the data subject. As a matter of best practice, the controller can also provide the data subject with the information from the *balancing test*, which must be carried out to allow reliance on Article 6.1(f) as a lawful basis for processing, in advance of any collection of data subjects’ personal data. To avoid information fatigue, this can be included within a layered privacy statement/notice (see paragraph 35). In any case, the WP29 position is that information to the data subject should make it clear that they can obtain information on the balancing test upon request. This is essential for effective transparency where data subjects have doubts as to whether the balancing test has been carried out fairly or they wish to file a complaint with a supervisory authority. |
| Categories of personal data concerned | Not required | Article 14.1(d) | This information is required in an Article 14 scenario because the personal data has not been obtained from the data subject, who therefore lacks an awareness of which categories of their personal data the data controller has obtained. |
| Recipients\(^6\) (or categories of recipients) of the personal data | Article 13.1(e) | Article 14.1(e) | The term “recipient” is defined in Article 4.9 as “a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not” [emphasis added]. As such, a recipient does not have to be a third party. Therefore, other data controllers, joint controllers and processors to whom data is transferred or disclosed are covered by the term “recipient” and information on such recipients should be provided in addition to information on third party recipients. The actual (named) recipients of the personal data, or the categories of recipients, must be provided. In accordance with the principle of fairness, controllers must provide information on the recipients that is most meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data. If controllers opt to provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients. |
| Details of transfers to third countries, the fact of same and the details of the relevant | Article 13.1(f) | Article 14.1(f) | The relevant GDPR article permitting the transfer and the corresponding mechanism (e.g. adequacy decision under Article 61 As defined by Article 4.9 of the GDPR and referenced in Recital 31 |

\(^6\) As defined by Article 4.9 of the GDPR and referenced in Recital 31.
safeguards\textsuperscript{62} (including the existence or absence of a Commission adequacy decision\textsuperscript{63}) and the means to obtain a copy of them or where they have been made available.

| The storage period (or if not possible, criteria used to determine that period) | Article 13.2(a) | Article 14.2(a) | 45/ binding corporate rules under Article 47/ standard data protection clauses under Article 46.2/ derogations and safeguards under Article 49 etc.) should be specified. Information on where and how the relevant document may be accessed or obtained should also be provided e.g. by providing a link to the mechanism used. In accordance with the principle of fairness, the information provided on transfers to third countries should be as meaningful as possible to data subjects; this will generally mean that the third countries be named.

---

\textsuperscript{62} As set out in Article 46.2 and 46.3

\textsuperscript{63} In accordance with Article 45
<table>
<thead>
<tr>
<th>Categories</th>
<th>Article</th>
<th>Article</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>The rights of the data subject to:</td>
<td>Article 13.2(b)</td>
<td>Article 14.2(c)</td>
<td>This information should be specific to the processing scenario and include a summary of what the right involves and how the data subject can take steps to exercise it and any limitations on the right (see paragraph 68 above). In particular, the right to object to processing must be explicitly brought to the data subject's attention at the latest at the time of first communication with the data subject and must be presented clearly and separately from any other information.64 In relation to the right to portability, see WP29 Guidelines on the right to data portability.65</td>
</tr>
<tr>
<td>Where processing is based on consent (or explicit consent), the right to withdraw consent at any time</td>
<td>Article 13.2(c)</td>
<td>Article 14.2(d)</td>
<td>This information should include how consent may be withdrawn, taking into account that it should be as easy for a data subject to withdraw consent as to give it.66</td>
</tr>
<tr>
<td>The right to lodge a complaint with a supervisory authority</td>
<td>Article 13.2(d)</td>
<td>Article 14.2(e)</td>
<td>This information should explain that, in accordance with Article 77, a data subject has the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or of an alleged infringement of the GDPR.</td>
</tr>
</tbody>
</table>
| Whether there is a statutory or contractual requirement to provide the information or whether it is necessary to | Article 13.2(e) | Not required                            | For example in an employment context, it may be a contractual requirement to provide certain information for the purposes of employment.

---

64 Article 21.4 and Recital 70 (which applies in the case of direct marketing)
65 Guidelines on the right to data portability, WP 242 rev.01, last revised and adopted on 5 April 2017
66 Article 7.3
enter into a contract or whether there is an obligation to provide the information and the possible consequences of failure.

<table>
<thead>
<tr>
<th>The source from which the personal data originate, and if applicable, whether it came from a publicly accessible source</th>
<th>Not required</th>
<th>Article 14.2(f)</th>
<th>The specific source of the data should be provided unless it is not possible to do so – see further guidance at paragraph 60. If the specific source is not named then information provided should include: the nature of the sources (i.e. publicly/privately held sources) and the types of organisation/industry/sector.</th>
</tr>
</thead>
<tbody>
<tr>
<td>The existence of automated decision-making including profiling and, if applicable, meaningful information about the logic used and the significance and envisaged consequences of such processing for the data subject</td>
<td>Article 13.2(f)</td>
<td>Article 14.2(g)</td>
<td>See WP29 Guidelines on automated individual decision-making and Profiling.67</td>
</tr>
</tbody>
</table>

---

67 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251
SEC. 2.

The Legislature finds and declares that:

(a) In 1972, California voters amended the California Constitution to include the right of privacy among the “inalienable” rights of all people. The amendment established a legal and enforceable right of privacy for every Californian. Fundamental to this right of privacy is the ability of individuals to control the use, including the sale, of their personal information.

(b) Since California voters approved the right of privacy, the California Legislature has adopted specific mechanisms to safeguard Californians’ privacy, including the Online Privacy Protection Act, the Privacy Rights for California Minors in the Digital World Act, and Shine the Light, a California law intended to give Californians the ‘who, what, where, and when’ of how businesses handle consumers’ personal information.

(c) At the same time, California is one of the world’s leaders in the development of new technologies and related industries. Yet the proliferation of personal information has limited Californians’ ability to properly protect and safeguard their privacy. It is almost impossible to apply for a job, raise a child, drive a car, or make an appointment without sharing personal information.

(d) As the role of technology and data in the everyday lives of consumers increases, there is an increase in the amount of personal information shared by consumers with businesses. California law has not kept pace with these developments and the personal privacy implications surrounding the collection, use, and protection of personal information.

(e) Many businesses collect personal information from California consumers. They may know where a consumer lives and how many children a consumer has, how fast a consumer drives, a consumer’s personality, sleep habits, biometric and health information, financial information, precise geolocation information, and social networks, to name a few categories.

(f) The unauthorized disclosure of personal information and the loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm.

(g) In March 2018, it came to light that tens of millions of people had their personal data misused by a data mining firm called Cambridge Analytica. A series of congressional hearings highlighted that our personal information may be vulnerable to misuse when shared on the Internet. As a result, our desire for privacy controls and transparency in data practices is heightened.

(h) People desire privacy and more control over their information. California consumers should be able to exercise control over their personal information, and they want to be certain that there are safeguards against misuse of their personal information. It is possible for businesses both to respect consumers’ privacy and provide a high level transparency to their business practices.

(i) Therefore, it is the intent of the Legislature to further Californians’ right to privacy by giving consumers an effective way to control their personal information, by ensuring the following rights:

1. The right of Californians to know what personal information is being collected about them.
2. The right of Californians to know whether their personal information is sold or disclosed and to whom.
3. The right of Californians to say no to the sale of personal information.
4. The right of Californians to access their personal information.
5. The right of Californians to equal service and price, even if they exercise their privacy rights.
SEC. 3.
Title 1.81.5 (commencing with Section 1798.100) is added to Part 4 of Division 3 of the Civil Code, to read:

TITLE 1.81.5. California Consumer Privacy Act of 2018

1798.100. (a) A consumer shall have the right to request that a business that collects a consumer’s personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.

(b) A business that collects a consumer’s personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

(c) A business shall provide the information specified in subdivision (a) to a consumer only upon receipt of a verifiable consumer request.

(d) A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.

(e) This section shall not require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

(1) Retain any personal information collected for a single, one-time transaction, if the information is not sold or retained by the business.

(2) Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

1798.105. (a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

(b) A business that collects personal information about consumers shall disclose, pursuant to subparagraph (A) of paragraph (5) of subdivision (a) of Section 1798.130, the consumer’s rights to request the deletion of the consumer’s personal information.

(c) A business that receives a verifiable consumer request from a consumer to delete the consumer’s personal information pursuant to subdivision (a) of this section shall delete the consumer’s personal information from its records and direct any service providers to delete the consumer’s personal information from their records.

(d) A business or a service provider shall not be required to comply with a consumer’s request to delete the consumer’s personal information if it is necessary for the business or service provider to maintain the consumer’s personal information in order to:

(1) Complete the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business’s ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

(2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.

(3) Debug to identify and repair errors that impair existing intended functionality.

(4) Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.
(5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.

(6) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the businesses’ deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

(7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer’s relationship with the business.

(8) Comply with a legal obligation.

(9) Otherwise use the consumer’s personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

1798.110. (a)
A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following:

(1) The categories of personal information it has collected about that consumer.

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting or selling personal information.

(4) The categories of third parties with whom the business shares personal information.

(5) The specific pieces of personal information it has collected about that consumer.

(b) A business that collects personal information about a consumer shall disclose to the consumer, pursuant to paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable consumer request from the consumer.

(c) A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The categories of personal information it has collected about that consumer.

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting or selling personal information.

(4) The categories of third parties with whom the business shares personal information.

(5) The specific pieces of personal information the business has collected about that consumer.

(d) This section does not require a business to do the following:

(1) Retain any personal information about a consumer collected for a single one-time transaction if, in the ordinary course of business, that information about the consumer is not retained.

(2) Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

1798.115. (a)
A consumer shall have the right to request that a business that sells the consumer’s personal information, or that discloses it for a business purpose, disclose to that consumer:

(1) The categories of personal information that the business collected about the consumer.

(2) The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold.

(3) The categories of personal information that the business disclosed about the consumer for a business purpose.
A business that sells personal information about a consumer, or that discloses a consumer’s personal information for a business purpose, shall disclose, pursuant to paragraph (4) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) to the consumer upon receipt of a verifiable consumer request from the consumer.

A business that sells consumers’ personal information, or that discloses consumers’ personal information for a business purpose, shall disclose, pursuant to subparagraph (C) of paragraph (5) of subdivision (a) of Section 1798.130:

- The category or categories of consumers’ personal information it has sold, or if the business has not sold consumers’ personal information, it shall disclose that fact.
- The category or categories of consumers’ personal information it has disclosed for a business purpose, or if the business has not disclosed the consumers’ personal information for a business purpose, it shall disclose that fact.

A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out pursuant to Section 1798.120.

1798.120. (a)
A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer’s personal information. This right may be referred to as the right to opt out.

(b) A business that sells consumers’ personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the “right to opt out” of the sale of their personal information.

(c) A business that has received direction from a consumer not to sell the consumer’s personal information or, in the case of a minor consumer’s personal information, has not received consent to sell the minor consumer’s personal information shall be prohibited, pursuant to paragraph (4) of subdivision (a) of Section 1798.135, from selling the consumer’s personal information after its receipt of the consumer’s direction, unless the consumer subsequently provides express authorization for the sale of the consumer’s personal information.

(d) Notwithstanding subdivision (a), a business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers between 13 and 16 years of age, or the consumer’s parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer’s personal information. A business that willfully disregards the consumer’s age shall be deemed to have had actual knowledge of the consumer’s age. This right may be referred to as the “right to opt in.”

(d) A business that has received direction from a consumer not to sell the consumer’s personal information or, in the case of a minor consumer’s personal information, has not received consent to sell the minor consumer’s personal information shall be prohibited, pursuant to paragraph (4) of subdivision (a) of Section 1798.135, from selling the consumer’s personal information after its receipt of the consumer’s direction, unless the consumer subsequently provides express authorization for the sale of the consumer’s personal information.

1798.125. (a)(1)
(a) A business shall not discriminate against a consumer because the consumer exercised any of the consumer’s rights under this title, including, but not limited to, by:

- Denying goods or services to the consumer.
- Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.
- Providing a different level or quality of goods or services to the consumer, if the consumer exercises the consumer’s rights under this title.
- Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.
(2) (2) Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer’s data.

(b) (b)

(1) (1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer’s data.

(2) (2) A business that offers any financial incentives pursuant to subdivision (a), shall notify consumers of the financial incentives pursuant to Section 1798.135.

(3) (3) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.135 which clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.

(4) (4) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

1798.130. (a) (a)

In order to comply with Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers, a business shall:

(1) (1) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, including, at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address.

(2) (2) Disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable consumer request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business’s duty to disclose and deliver the information within 45 days of receipt of the consumer’s request. The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure shall cover the 12-month period preceding the business’s receipt of the verifiable consumer request and shall be made in writing and delivered through the consumer’s account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer’s option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business shall not require the consumer to create an account with the business in order to make a verifiable consumer request.

(3) (3) For purposes of subdivision (b) of Section 1798.110:

(A) (A) To identify the consumer, associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) (B) Identify by category or categories the personal information collected about the consumer in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected.

(4) (4) For purposes of subdivision (b) of Section 1798.115:

(A) (A) Identify the consumer and associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) (B) Identify by category or categories the personal information of the consumer that the business sold in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer’s personal information was sold in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information sold. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (C).

(C) (C) Identify by category or categories the personal information of the consumer that the business disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely
describes the personal information, and provide the categories of third parties to whom the consumer’s personal information was disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information disclosed. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (B).

(5) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers’ privacy rights, or if the business does not maintain those policies, on its Internet Web site, and update that information at least once every 12 months:

(A) A description of a consumer’s rights pursuant to Sections 1798.110, 1798.115, and 1798.125 and one or more designated methods for submitting requests.

(B) For purposes of subdivision (c) of Section 1798.110, a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.

(C) For purposes of paragraphs (1) and (2) of subdivision (c) of Section 1798.115, two separate lists:

(i) A list of the categories of personal information it has sold about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information sold, or if the business has not sold consumers’ personal information in the preceding 12 months, the business shall disclose that fact.

(ii) A list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describe the personal information disclosed, or if the business has not disclosed consumers’ personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(6) Ensure that all individuals responsible for handling consumer inquiries about the business’s privacy practices or the business’s compliance with this title are informed of all requirements in Sections 1798.110, 1798.115, 1798.125, and this section, and how to direct consumers to exercise their rights under those sections.

(7) Use any personal information collected from the consumer in connection with the business’s verification of the consumer’s request solely for the purposes of verification.

(b) A business is not obligated to provide the information required by Sections 1798.110 and 1798.115 to the same consumer more than twice in a 12-month period.

(c) The categories of personal information required to be disclosed pursuant to Sections 1798.110 and 1798.115 shall follow the definition of personal information in Section 1798.140.

1798.135. (a)

A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers:

(1) Provide a clear and conspicuous link on the business’s Internet homepage, titled “Do Not Sell My Personal Information,” to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer’s personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer’s personal information.

(2) Include a description of a consumer’s rights pursuant to Section 1798.120, along with a separate link to the “Do Not Sell My Personal Information” Internet Web page in:

(A) Its online privacy policy or policies if the business has an online privacy policy or policies.

(B) Any California-specific description of consumers’ privacy rights.

(3) Ensure that all individuals responsible for handling consumer inquiries about the business’s privacy practices or the business’s compliance with this title are informed of all requirements in Section 1798.120 and this section and how to direct consumers to exercise their rights under those sections.

(4) For consumers who exercise their right to opt-out of the sale of their personal information, refrain from selling personal information collected by the business about the consumer.

(5) For a consumer who has opted-out of the sale of the consumer’s personal information, respect the consumer’s decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer’s personal information.
(6) (a) Use any personal information collected from the consumer in connection with the submission of the consumer’s opt-out request solely for the purposes of complying with the opt-out request.

(b) Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.

(c) (a) A consumer may authorize another person solely to opt-out of the sale of the consumer’s personal information on the consumer’s behalf, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer’s behalf, pursuant to regulations adopted by the Attorney General.

1798.140.

For purposes of this title:

(a) “Aggregate consumer information” means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. “Aggregate consumer information” does not mean one or more individual consumer records that have been de-identified.

(b) “Biometric information” means an individual’s physiological, biological or behavioral characteristics, including an individual’s deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(c) “Business” means:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers’ personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers’ personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys, receives for the business’s commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.

(C) Derives 50 percent or more of its annual revenues from selling consumers’ personal information.

(2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business. “Control” or “controlled” means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. “Common branding” means a shared name, servicemark, or trademark.

(d) “Business purpose” means the use of personal information for the business’s or a service provider’s operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed for or another operational purpose that is compatible with the context in which the personal information was collected. Business purposes are:

(1) Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

(2) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.
“Commercial purposes” means to advance a person’s commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. “Commercial purposes” do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.

“Consumer” means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

“Deidentified” means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

1. Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
2. Has implemented business processes that specifically prohibit reidentification of the information.
3. Has implemented business processes to prevent inadvertent release of deidentified information.
4. Makes no attempt to reidentify the information.
5. “Designated methods for submitting requests” means a mailing address, email address, Internet Web page, Internet Web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185.
6. “Device” means any physical object that is capable of connecting to the Internet, directly or indirectly, or to another device.
7. “Health insurance information” means a consumer’s insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the consumer, or any information in the consumer’s application and claims history, including any appeals records, if the information is linked or reasonably linkable to a consumer or household, including via a device, by a business or service provider.
8. “Homepage” means the introductory page of an Internet Web site and any Internet Web page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application’s platform page or download page, a link within the application, such as from the application configuration, “About,” “Information,” or settings page, and any other location that allows consumers to review the notice required by subdivision (a) of Section 1798.145, including, but not limited to, before downloading the application.
9. “Infer” or “inference” means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.
10. “Person” means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in
(a) “Personal information” means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers.

(B) Any categories of personal information described in subdivision (e) of Section 1798.80.

(C) Characteristics of protected classifications under California or federal law.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer’s interaction with an Internet Web site, application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

(I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g. 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(2) “Personal information” does not include publicly available information. For these purposes, “publicly available” means information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information. “Publicly available” does not mean biometric information collected by a business about a consumer without the consumer’s knowledge. Information is not “publicly available” if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained. “Publicly available” does not include consumer information that is deidentified or aggregate consumer information.

(p) “Probabilistic identifier” means the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.

(q) “Processing” means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means.

(r) “Pseudonymize” or “Pseudonymization” means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

(s) “Research” means scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer’s interactions with a business’s service or device for other purposes shall be:

(1) Compatible with the business purpose for which the personal information was collected.

(2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.
Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

Subject to business processes that specifically prohibit reidentification of the information.

Made subject to business processes to prevent inadvertent release of deidentified information.

Protected from any reidentification attempts.

Used solely for research purposes that are compatible with the context in which the personal information was collected.

Not be used for any commercial purpose.

Subjected by the business conducting the research to additional security controls limit access to the research data to only those individuals in a business as are necessary to carry out the research purpose.

For purposes of this title, a business does not sell personal information when:

A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer’s intent to interact with a third party.

The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer’s personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer’s personal information.

The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met: services that the service provider performs on the business’ behalf, provided that the service provider also does not sell the personal information.

The business has provided notice that information being used or shared in its terms and conditions consistent with Section 1798.135.

The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with Sections 1798.110 and 1798.115. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with Section 1798.120. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

“Service” or “services” means work, labor, and services, including services furnished in connection with the sale or repair of goods.

A “service provider” means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer’s personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.
Third party means a person who is not any of the following:

1. The business that collects personal information from consumers under this title.

2. A person to whom the business discloses a consumer’s personal information for a business purpose pursuant to a written contract, provided that the contract:
   - Prohibits the person receiving the personal information from:
     - Selling the personal information.
     - Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.
     - Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.
   - Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.

A person covered by this paragraph (2) that violates any of the restrictions set forth in this title shall be liable for the violations. A business that discloses personal information to a person covered by this paragraph (2) in compliance with this paragraph (2) shall not be liable under this title if the person receiving the personal information uses it in violation of the restrictions set forth in this title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation.

Unique identifier or Unique personal identifier means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, “family” means a custodial parent or guardian and any minor children over which the parent or guardian has custody.

Verifiable consumer request means a request that is made by a consumer, by a consumer on behalf of the consumer’s minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer’s behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.110 and 1798.115 if the business cannot verify, pursuant this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer’s behalf.

1798.145. (a)

The obligations imposed on businesses by this title shall not restrict a business’s ability to:

1. Comply with federal, state, or local laws.
2. Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.
3. Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.
4. Exercise or defend legal claims.
5. Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.
6. Collect or sell a consumer’s personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer’s personal
information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not permit a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.

(b) The obligations imposed on businesses by Sections 1798.110 to 1798.135, inclusive, shall not apply where compliance by the business with the title would violate an evidentiary privilege under California law and shall not prevent a business from providing the personal information of a consumer to a person covered by an evidentiary privilege under California law as part of a privileged communication.

(c) This title shall not apply to any of the following:

(1) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5). (B) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section.

(2) Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration.

(3) This title shall not apply to the sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report as defined by subdivision (d) of Section 160.103 of Title 45 of the Code of Federal Regulations.

(d) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, if it is in conflict with that law or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code).

(e) Notwithstanding a business’s obligations to respond to and honor consumer rights requests pursuant to this title:

(1) A time period for a business to respond to any verified consumer request may be extended by up to 90 additional days where necessary, taking into account the complexity and number of the requests. The business shall inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.

(2) If the business does not take action on the request of the consumer, the business shall inform the consumer, without delay and at the latest within the time period permitted of response by this section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business.

(3) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the burden of demonstrating that any verified consumer request is manifestly unfounded or excessive.

(h) A business that discloses personal information to a service provider shall not be liable under this title if the service
provider receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the
time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service
provider intends to commit such a violation. A service provider shall likewise not be liable under this title for the obligations
of a business for which it provides services as set forth in this title.

\( i \) \( (i) \) This title shall not be construed to require a business to reidentify or otherwise link information that is not maintained
in a manner that would be considered personal information.

\( ii \) \( (ii) \) The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the
rights and freedoms of other consumers.

\( k \) The rights afforded to consumers and the obligations imposed on any business under this title shall not apply to the extent
that they infringe on the noncommercial activities of a person or entity described in subdivision (b) of Section 2 of Article I of
the California Constitution.

1798.150. \((a)(1)\)

\( a \)

\( 1 \) Any consumer whose nonencrypted or nonredacted personal information, as defined in subparagraph (A) of paragraph (1)
of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of
the business’s violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the
nature of the information to protect the personal information may institute a civil action for any of the following:

\( A \) \( (A) \) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and
fifty ($750) per consumer per incident or actual damages, whichever is greater.

\( B \) \( (B) \) Injunctive or declaratory relief.

\( C \) \( (C) \) Any other relief the court deems proper.

\( 2 \) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances
presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the
number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the
willfulness of the defendant’s misconduct, and the defendant’s assets, liabilities, and net worth.

\( b \)

\( 1 \) Actions pursuant to this section may be brought by a consumer if all of the following requirements are met: \( (1) \) Prior
to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer shall
provide a business 30 days’ written notice identifying the specific provisions of this title the consumer alleges have been or are
being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides
the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action
for individual statutory damages or class-wide statutory damages may be initiated against the business. No notice shall
be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged
violations of this title. If a business continues to violate this title in breach of the express written statement
provided to the consumer under this section, the consumer may initiate an action against the business to
enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as
any other violation of the title that postdates the written statement.

\( 2 \) A consumer bringing an action The cause of action established by this section shall apply only to violations as defined
in paragraph (1) of subdivision (c) shall notify the Attorney General within 30 days that the action has been filed.

\( 3 \) The Attorney General, upon receiving such notice shall, within 30 days, do one of the following:

\( A \) Notify the consumer bringing the action of the Attorney General’s intent to prosecute an action against the violation. If
the Attorney General does not prosecute within six months, the consumer may proceed with the action.

\( B \) Refrain from acting within the 30 days, allowing the consumer bringing the action to proceed.

\( C \) Notify the consumer bringing the action that the consumer shall not proceed with the action. Nothing in this
act subdivision (a) and shall not be based on violations of any other section of this title. Nothing in this title shall be
interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any
party from any duties or obligations imposed under other law or the United States or California Constitution.
1798.155.

(a) Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title.

(b) A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty as provided in Section 17206 of the Business and Professions Code of not more than five thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General. The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.

(b) Notwithstanding Section 17206 of the Business and Professions Code, any person, business, or service provider that intentionally violates this title may be liable for a civil penalty of up to seven thousand five hundred dollars ($7,500) for each violation.

(b) (c) Notwithstanding Section 17206 of the Business and Professions Code, any civil penalty assessed pursuant to Section 17206 for a violation of this title, and the proceeds of any settlement of an action brought pursuant to subdivision (b), shall be allocated as follows: (1) Twenty percent to be deposited in the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.109, 1798.175 with the intent to fully offset any costs incurred by the state courts and the Attorney General in connection with this title.

(2) Eighty percent to the jurisdiction on whose behalf the action leading to the civil penalty was brought.

(d) It is the intent of the Legislature that the percentages specified in subdivision (c) be adjusted as necessary to ensure that any civil penalties assessed for a violation of this title fully offset any costs incurred by the state courts and the Attorney General in connection with this title, including a sufficient amount to cover any deficit from a prior fiscal year.

1798.160. (a)

(a) A special fund to be known as the “Consumer Privacy Fund” is hereby created within the General Fund in the State Treasury, and is available upon appropriation by the Legislature to offset any costs incurred by the state courts in connection with actions brought to enforce this title and any costs incurred by the Attorney General in carrying out the Attorney General’s duties under this title.

(b) (b) Funds transferred to the Consumer Privacy Fund shall be used exclusively to offset any costs incurred by the state courts and the Attorney General in connection with this title. These funds shall not be subject to appropriation or transfer by the Legislature for any other purpose, unless the Director of Finance determines that the funds are in excess of the funding needed to fully offset the costs incurred by the state courts and the Attorney General in connection with this title, in which case the Legislature may appropriate excess funds for other purposes.

1798.175.

This title is intended to further the constitutional right of privacy and to supplement existing laws relating to consumers’ personal information, including, but not limited to, Chapter 22 (commencing with Section 22575) of Division 8 of the Business and Professions Code and Title 1.81 (commencing with Section 1798.80). The provisions of this title are not limited to information collected electronically or over the Internet, but apply to the collection and sale of all personal information collected by a business from consumers. Wherever possible, law relating to consumers’ personal information should be construed to harmonize with the provisions of this title, but in the event of a conflict between other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.

1798.180.

This title is a matter of statewide concern and supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the collection and sale of consumers’ personal information by a business.
On or before January 1, 2020, the Attorney General shall solicit broad public participation to adopt regulations to further the purposes of this title, including, but not limited to, the following areas:

(a) Adjusting as needed additional categories of personal information to those enumerated in subdivision (c) of Section 1798.130 and subdivision (o) of Section 1798.140 in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.

(b) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.

(c) Establishing rules and procedures for the following, within one year of passage of this title and as needed thereafter:

(A) Implementing Section 1798.130 to ensure that businesses provide notice of consumer rights at or with the first consumer interaction, and shall not wait until the business sends the notice.

(B) Establishing rules and procedures for the following, within one year of passage of this title and as needed thereafter:

(a) The development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.

(b) The Attorney General may adopt additional regulations as necessary to further the purposes of this title.

(4) The Attorney General shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner.

If a series of steps or transactions were component parts of a single transaction intended from the beginning to be taken with the intention of avoiding the reach of this title, including the disclosure of information by a business to a third party in order to avoid the definition of sell, a court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title.

Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer’s rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable. This section shall not prevent a consumer from declining to request information from a business, declining to opt-out of a business’s sale of the consumer’s personal information, or authorizing a business to sell the consumer’s personal information after previously opting out.
1798.194.
This title shall be liberally construed to effectuate its purposes.

1798.196.
This title is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the United States or California Constitution.

1798.198. (a)
Subject to limitation provided in subdivision (b), and in Section 1798.199, this title shall be operative January 1, 2020.

(b) This title shall become operative only if initiative measure No. 17-0039, The Consumer Right to Privacy Act of 2018, is withdrawn from the ballot pursuant to Section 9604 of the Elections Code.

1798.199.
Notwithstanding Section 1798.198, Section 1798.180 shall be operative on the effective date of the act adding this section.

SEC. 4. (a)
The provisions of this bill are severable. If any provision of this bill or its application is held invalid, that invalidity shall not affect other provisions or applications that can be given effect without the invalid provision or application.
## Document comparison by Workshare 9.5 on Monday, December 3, 2018 5:03:57 PM

### Input:

<table>
<thead>
<tr>
<th>Document 1 ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>file://\nyc-us-file-01\Users\jdrucker\Documents\CCPA - Original Text.docx</td>
<td>CCPA - Original Text</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Document 2 ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interwovenSite://LOCAL/US/136751826/2</td>
<td>#136751826v2&lt;US&gt; - CCPA - Updated by SB1121</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rendering set</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Firm Word - Show moves, Adds Double Underline, Delete Strikethrough</td>
<td></td>
</tr>
</tbody>
</table>

### Legend:

- **Insertion**
- **Deletion**
- **Moved from**
- **Moved to**
- **Style change**
- **Format change**
- **Moved deletion**
- **Inserted cell**
- **Deleted cell**
- **Moved cell**
- **Split/Merged cell**
- **Padding cell**

### Statistics:

<table>
<thead>
<tr>
<th></th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insertions</td>
<td>330</td>
</tr>
<tr>
<td>Deletions</td>
<td>271</td>
</tr>
<tr>
<td>Moved from</td>
<td>2</td>
</tr>
<tr>
<td>Moved to</td>
<td>2</td>
</tr>
<tr>
<td>Style change</td>
<td>0</td>
</tr>
<tr>
<td>Format changed</td>
<td>0</td>
</tr>
<tr>
<td>Total changes</td>
<td>605</td>
</tr>
</tbody>
</table>