

CONTENTS

ABOUT THE AUTHOR	XIX
NOTES ON CITATIONS	XXI
ACKNOWLEDGMENTS	XXIII
INTRODUCTION	XXV
GENERAL CONCEPTS	1
Q.1 What is a data “controller”?	1
Q.2 What is a data “processor”?	1
Q.3 What activities count as “processing”?	2
Q.4 What is “personal data”?	2
Q.5 Do the terms “personal data,” “personal information,” and “personally identifiable information” mean the same thing?	3
Q.6 What is a “data subject”?	4
JURISDICTION	5
Q.7 What does it mean to be “established” in the European Union?	5
Q.8 Does the GDPR apply to a company that has no employees or offices in the European Union?	7
Q.9 If a company is not “established” in the European Union, does it have to have a registered agent that is within the European Economic Area?	8
Q.10 What is the maximum penalty for failing to appoint a representative (if one is required)?	10

Q.11 Does the GDPR apply equally to all countries within the European Economic Area? **10**

Q.12 When did the GDPR become law? **10**

SCOPE **13**

Q.13 Can a service provider become a “controller”? **13**

Q.14 Does the GDPR impart the same requirements on controllers and processors? **13**

Q.15 Does the GDPR apply to all controllers and processors? **14**

Q.16 Does the GDPR apply to 501(c)(3) nonprofits? **14**

Q.17 Does the GDPR apply only to European Union citizens’ data? **15**

Q.18 Can the GDPR apply to personal data about United States citizens? **16**

Q.19 Are work e-mail addresses and business contact information considered “personal data”? **16**

Q.20 Is an IP address considered “personal data”? **17**

Q.21 Is a cookie considered “personal data”? **18**

Q.22 Does the GDPR apply to paper records? **18**

Q.23 What is “anonymized” data? **20**

Q.24 Is there an approved technique for anonymizing data under the GDPR? **20**

Q.25 What is “pseudonymized” data? **20**

Q.26 Is it possible for data that has undergone hashing to still be considered “personal data”? **21**

Q.27 Is it possible for data that has undergone salted-hashing to still be considered “personal data”? **21**

Q.28 Is encrypted data out of the scope of the GDPR? **22**

Q.29 Does the GDPR apply to information about businesses? **22**

CONSENT AND USING DATA	23
Q.30 Are companies always required by the GDPR to get opt-in consent before using personal data?	23
Q.31 Are companies always required to get opt-in consent from people before using their data for direct marketing?	25
Q.32 Does the GDPR require that a company obtain consent from a website user before placing cookies on its browser?	25
Q.33 Does a company need to get employees' consent to collect information from them?	26
Q.34 Does a company need employees' consent to monitor them?	27
Q.35 Are there any situations in which a company can base processing of employee information upon consent?	27
Q.36 What requirements does the GDPR impose upon a company that attempts to get consent?	28
Q.37 Can a company use a prechecked box when collecting consent?	29
PRIVACY POLICIES/INFORMATION NOTICES	31
Q.38 What is a privacy notice?	31
Q.39 If a company drafted a privacy notice to comply with United States laws, does it need to change the notice to comply with the GDPR?	31
Q.40 Does a company always have to provide a privacy notice to people from whom it collects information?	34
Q.41 Do companies always have to provide a privacy notice if they collect personal data from a third party?	35
Q.42 Does a company need to translate its privacy notice into other languages?	36

Q.43 What is the maximum penalty if a privacy notice does not comply with the GDPR?	36
AN INDIVIDUAL'S RIGHT TO BE FORGOTTEN	39
Q.44 What is the "right to be forgotten"?	39
Q.45 Did the GDPR create the right to be forgotten?	39
Q.46 Are there any analogs to the right to be forgotten within United States law?	40
Q.47 Are all companies required to create a policy or procedure for processing right to be forgotten requests?	40
Q.48 What do most companies include in a right to be forgotten policy or procedure?	41
Q.49 If a company receives a right to be forgotten request, does it always have to delete the requestor's information?	42
Q.50 If a company receives a right to be forgotten request from an employee or a former employee, does it have to delete the requestor's information?	45
Q.51 When honoring a right to be forgotten request, does a company have to delete the person's information from all of its backup systems?	47
Q.52 If a company receives a right to be forgotten request from a former employee who was terminated for cause, does it have to delete information about their performance and the termination event?	49
Q.53 If a company receives a right to be forgotten request, does it have to delete the request itself?	51
Q.54 If a company receives a right to be forgotten request from a client who is an individual with a current contract for a product or service, what should it do?	52
Q.55 Can a company charge a fee for responding to a right to be forgotten request?	53

Q.56 How much time does a company have to respond to a right to be forgotten request?	54
Q.57 What is the maximum penalty for violating an individual's right to be forgotten?	54
AN INDIVIDUAL'S RIGHT TO ACCESS THEIR INFORMATION	55
Q.58 What is the "right to access"?	55
Q.59 Did the GDPR create the right of access?	55
Q.60 How far can a company go to validate the identity of an individual making a data subject access request?	55
Q.61 If a company receives a data access request from a former employee, does it have to share with that employee performance reviews and other notes and comments in their HR file?	57
Q.62 Are all companies required to create a policy or procedure for processing access requests?	58
Q.63 What do most companies include in a data access policy or procedure?	59
Q.64 Are there any analogs to the right of access in the United States?	60
Q.65 What is the maximum penalty for violating an individual's right to access their information?	60
AN INDIVIDUAL'S RIGHT TO RECEIVE INFORMATION IN A PORTABLE FORMAT	61
Q.66 Does a company always have to respond to a data subject's request to receive access to their information by providing it in a "portable" format?	61
Q.67 If a company is required to provide data in a "portable" format, what file types can it use?	62
Q.68 How much time does a company have to respond to a data portability request?	64

Q.69 Can a company charge a fee for responding to a data portability request?	64
AN INDIVIDUAL'S RIGHT TO FIX THEIR INFORMATION	67
Q.70 What is the "right of rectification"?	67
Q.71 Are all companies required to create a policy or procedure for processing rectification requests?	67
Q.72 How much time does a company have to respond to a rectification request?	68
DOCUMENT RETENTION	71
Q.73 What is "data minimization"?	71
Q.74 Do all companies need to implement a records retention policy?	71
Q.75 If a company already has a records retention policy, does it need to be updated in light of the GDPR?	72
Q.76 How detailed does a company's records retention periods have to be to satisfy the GDPR?	72
RECORD KEEPING	75
Q.77 Are controllers required to do a "data inventory"?	75
Q.78 Are processors required to do a "data inventory"?	76
Q.79 Does the GDPR provide a template "data inventory" for companies to use?	76
Q.80 Are small businesses required to keep the same records of compliance as large businesses?	77
Q.81 What is the maximum penalty if a company does not create all of the records required by the GDPR?	78

Q.82 What written policies and procedures do companies typically create to demonstrate their compliance with the GDPR?	78
GOVERNANCE	81
Q.83 Are all companies required to have a Data Protection Officer?	81
Q.84 What does “large scale” mean when determining whether a Data Protection Officer is necessary?	81
Q.85 If a company has a large number of employees, does it need to appoint a Data Protection Officer?	82
Q.86 If a company is required to have a Data Protection Officer, does that person have to be an employee of the organization?	83
Q.87 Does a Data Protection Officer have to be a lawyer?	84
Q.88 What does a Data Protection Officer have to do?	85
Q.89 What qualifications must a Data Protection Officer have?	87
Q.90 What is the maximum penalty for failing to appoint a Data Protection Officer (if one is required)?	88
DATA SECURITY	89
Q.91 Does the GDPR require that a company comply with a specific security standard?	89
Q.92 Is the GDPR’s data security standard new?	89
Q.93 Does the data security requirement within the GDPR apply to controllers or processors?	90
Q.94 If a company complies with United States laws concerning data security, is it also compliant with the GDPR’s data security requirements?	90

DATA BREACHES	91
Q.95 Does the GDPR require that controllers notify impacted people if there is a data breach?	91
Q.96 Does the GDPR require that controllers notify regulators if there is a data breach?	91
Q.97 Does the GDPR data breach notification provision cover the same type of data as United States data breach notification laws?	91
Q.98 Does the GDPR data breach notification provision only apply when personal data is accessed or acquired by an unauthorized third party?	92
Q.99 Does a company need to notify regulators every time it suffers a data breach?	93
Q.100 Is a company required to document data breaches?	93
Q.101 When does a company become “aware” of a data breach?	95
Q.102 Does a company need to notify impacted individuals every time it suffers a data breach?	95
Q.103 What information does a company have to include in the notices that it provides to individuals following a data breach?	96
Q.104 Is a processor required to notify a controller in the event of a data breach?	96
Q.105 Is a processor required to notify data protection authorities in the event of a data breach?	96
Q.106 Is a processor required to notify impacted individuals in the event of a data breach?	97
Q.107 How fast must a processor notify a controller?	97
Q.108 Does a controller’s time period for notifying a supervisory authority begin to run when its processor discovers a breach?	97

Q.109 Do service providers have to notify their clients about “suspected” breaches?	98
Q.110 Does the GDPR require that a company hire an external forensic investigator if it suspects a data breach?	98
Q.111 Does the GDPR require that a company provide credit restoration services following a data breach?	99
Q.112 If a company has an existing incident response plan, what provisions should it add in order to take into account the GDPR?	99
Q.113 What is the maximum penalty for failing to report a data breach within 72 hours?	101
TRANSFERRING DATA OUTSIDE OF THE EUROPEAN ECONOMIC AREA	103
Q.114 What is a “data exporter”?	103
Q.115 What is a “data importer”?	103
Q.116 Are companies allowed to transfer personal data outside of the European Economic Area?	103
Q.117 What does a company need to do to transfer data from an office in the European Economic Area to one of its offices or affiliates in the United States?	105
Q.118 If a company has a server located outside of the European Economic Area that holds personal data about Europeans, does that constitute a data transfer?	106
Q.119 After Brexit, can a company continue to transfer data from the European Union to the United Kingdom?	106
Q.120 When a European Union data subject transmits data directly to a United States company, is an adequacy measure required?	106

Q.121 Does the GDPR require that a company register model contract clauses with relevant supervisory authorities?	107
Q.122 Is there more than one set of “standard contractual clauses”?	108
Q.123 What is the difference between “Set 1” and “Set 2” of the Standard Contractual Clauses for transfers between controllers?	108
Q.124 Is there a set of Standard Contractual Clauses that can be used by a processor within the European Economic Area to send data to a subprocessor that is outside of the European Economic Area?	110
Q.125 What is the most popular method by which companies transfer data from the European Economic Area to the United States?	110
Q.126 How can a processor in the European Union transmit personal data to a subprocessor outside of the European Union without the use of a processor-processor Standard Contractual Clause?	111
Q.127 Should a company ask its employees to consent to transferring their information to the United States?	112
Q.128 If a company joins the EU-U.S. Privacy Shield Framework, is it agreeing to handle privacy-related disputes with consumers in a special way?	112
Q.129 If a company joins the European Union-United States Privacy Shield Framework, is it agreeing to handle privacy-related disputes with employees in a special way?	114
Q.130 Is the “Privacy Shield” the same thing as the “Safe Harbor”?	115

Q.131 Does the Privacy Shield and the Controller-Controller Set 2 Standard Contractual Clauses impose the same legal obligations upon a company in the United States?	115
Q.132 Does a company need to do anything in order to centralize its United States' employee records in the European Union?	120
Q.133 Does a company need to do anything in order to centralize its European employee records in the United States?	120
Q.134 Do the Privacy Shield and the Standard Contractual Clauses for transfers between controllers and processors impose the same legal obligations upon a company in the United States?	121
SERVICE PROVIDERS	127
Q.135 Are all service providers considered to be "processors"?	127
Q.136 What guarantees must a service provider that is acting as a processor provide to its controller client?	127
Q.137 When would a service provider be a "controller"?	129
Q.138 Should a service provider agreement explicitly state that the service provider is a "processor"?	130
Q.139 Does a controller have to dictate what software, hardware, and subcontractors its service providers use?	131
Q.140 If a service provider has already agreed to the controller-processor Standard Contractual Clauses, is a company required to put additional GDPR protections in place?	132

Q.141 If a service provider has self-certified to Privacy Shield, is a controller required to put additional GDPR protections in place?	137
Q.142 What is a “Data Protection Addendum”?	143
Q.143 Must the GDPR requirements for processors be included within the contractual agreement between a controller and a processor?	143
Q.144 If a data subject submits an access, rectification, or deletion request directly to a service provider, is the service provider required to respond to the data subject?	144
FINES	145
Q.145 Do all violations of the GDPR result in a fine of 4% of revenue?	145
Q.146 Can the European Data Protection Board assess fines?	146
Q.147 Is there a private right of action under the GDPR?	146
Q.148 Can a private plaintiff recover 4% of my gross revenue?	146
Q.149 Are there criminal penalties for violating the GDPR?	147
FINDING FURTHER GUIDANCE	149
Q.150 What is a “supervisory authority”?	149
Q.151 What agencies are authorized to interpret the GDPR?	149
Q.152 Where are cases under the GDPR filed?	150
Q.153 What is the Article 29 Working Party?	151
Q.154 What is the European Data Protection Board?	151
Q.155 Is the GDPR the source of European Union data privacy and security rights?	152

SPECIFIC SITUATIONS	153
Q.156 What are the main requirements that the GDPR imposes when a company collects general business contact information?	153
Q.157 What are the main requirements that the GDPR imposes when a company collects information from its employees?	155
Q.158 Does the GDPR overlap with the Gramm-Leach-Bliley Act?	157
Q.159 Does the GDPR overlap with the Health Insurance Portability and Accountability Act?	159
APPENDIX A	161
APPENDIX B	317
APPENDIX C	323
APPENDIX D	325
TABLE OF AUTHORITIES	343
INDEX	349