

# Table of Contents

<i>Table of Authorities</i>	xvii
<i>List of Abbreviations</i>	xxiii

Introduction: The risk-based approach as the opposite of the rights-based approach, or as an opportunity to analyse the links between law, regulation, and risk?	1
1. The risk-based approach: a contradiction in terms?	1
2. On the links between law and regulation	5
3. On data protection as regulation	7
4. The links between risk and regulation: the role of the proportionality principle	9
4.1 The proportionality principle as the missing link between law/regulation and risk	9
4.2 Defining the proportionality principle: two balancing tests associated with risk mitigation measures/safeguards	10
4.2.1 Risk mitigation or safeguards?	11
4.2.2 Proportionality as two balancing tests	12
4.2.3 Test 1: pressing social need	13
4.2.4 Test 2: proportionality <i>stricto sensu</i>	14
5. Proportionality as the common root of law/regulation and risk: some first lessons	15
5.1 Proportionality at the core of regulation and risk: closely intertwined practices	16
5.2 Proportionality as the hallmark of regulatory law: what consequences for data protection?	16
6. Approaching variations	18
7. Structure of the argument	24
1. Fundamental notions: Risk and regulation	26
1. Introduction	26
2. Risk	27
2.1 Etymology and meaning of the concept	27
2.2 Risk and risk management	28
2.3 The technique of risk and risk management	29
2.4 Risk (management) as a matter of two balancing tests associated to risk mitigation measures	31
2.5 Different methods for assessing risks	32
2.6 Different ways to manage risks	33
2.6.1 Risk management as an exercise in standard setting	33

2.6.2	How to balance the costs and benefits	34
2.6.3	The choice of the best risk mitigation measures	34
2.7	Challenges to risk management: beyond objectivity	37
2.7.1	Rise of risk analysis	37
2.8	Beyond risk analysis: sketching contemporary practices of risk management	40
3.	Regulation	41
3.1	Defining regulation	41
3.2	Regulation and law	42
3.2.1	Regulation, more than an economic concept	42
3.2.2	The characteristics of regulatory law	44
3.3	The object of regulation: harms	46
3.4	Studying the constitutive elements of regulation more in depth	48
3.4.1	Standard setting	48
3.4.2	Monitoring and behaviour control	48
3.4.3	Redefining the opposition between monitoring and behaviour control types of safeguards	49
3.4.4	The difference between enforcement and safeguards	51
4.	Risk and regulation as variations on the proportionality principle: a grid's eye view	52
2.	Data protection as command and control regulation	54
1.	Introduction: data protection as command and control regulation	54
2.	Data protection and standard setting	55
2.1	Data quality and legitimacy principles embody standard setting in data protection, and more in particular performance standards	56
2.2	Article 7: data legitimacy as the first balancing test	57
2.2.1	Data legitimacy is both about the legitimacy of the processing operation and its necessity	57
2.2.2	Data legitimacy in practice (1): presumptions	58
2.2.3	Data legitimacy in practice (2): <i>Heinz Huber</i>	59
2.2.4	Comparison with other views that do not support the existence of the first balancing test within data protection legislations	61
2.3	Article 6: data quality	64
2.3.1	Article 6(1)(c) as the embodiment of the second balancing test	64
2.3.2	Safeguard 1 = Transparency: principle of lawfulness, fairness and transparency + principle of purpose limitation	66
2.3.3	Safeguard 2 = Lawfulness, fairness, and legitimacy: principle of lawfulness, fairness and transparency + principle of purpose limitation	66
2.3.4	Safeguard 3 = reduction in scope: purpose limitation, data minimisation, storage limitation principles	67
2.3.5	Safeguard 4 = accuracy of the data: data accuracy principle	68
2.3.6	Safeguard 5 = security: principle of integrity and confidentiality	69
2.4	Data protection, standard setting, and proportionality: conclusions	69



3. Formal safeguards	70
3.1 Formal safeguards (1): deferred control	70
3.1.1 Advance determination and corrective intervention	70
3.1.2 Advance determination in data protection: licence, notification/registration, and prior checking	71
3.1.3 Advance determination as a good example as to why the distinction between monitoring and behaviour modification is of little relevance	72
3.1.4 Corrective intervention: the data protection authorities' powers	73
3.2 Formal safeguards (2): regulation through organisation	74
3.3 Formal safeguards (3): beyond the Data Protection Directive	75
3.3.1 Facilities v requirements	75
3.3.2 Regulation by classification	75
3.4 Formal safeguards (4): beyond Freund's classification: data subject rights	75
3.4.1 Data subject rights as safeguards: formal safeguards of deferred control	75
3.4.2 Data subject's right to be informed (Arts 10 and 11): advance determination	76
3.4.3 Rights of access and to object: corrective intervention	76
4. Substantive safeguards	78
5. Safeguards and data legitimacy	79
5.1 Presumption: the main safeguard	80
5.2 Consent	80
5.2.1 Consent as a safeguard in data protection	80
5.2.2 Consent as a safeguard in other fields	82
5.2.3 Consent as advance determination: prior approval, and transparency	83
5.3 The legitimate interests of the data controller	83
6. Enforcement	84
7. Conclusions: data protection as command and control regulation and the proportionality principle	84
3. Issues with data protection as command and control regulation	87
1. Introduction: data protection and issues with command and control regulation	87
2. Issues resulting from the "diagnosis-prescription" aspect of command and control regulation	89
3. Issues revolving around enforcement	92
4. List of challenges related to evolutions in data processing practices	94
5. Command and control issues at the data protection level	96
5.1 Inefficiency of the data protection core principles/congruence	96
5.2 Uncertainty/lack of clarity, predictability, transparency	98
5.3 Simplicity and accessibility	101

5.4 Enforcement	106
5.4.1 Under enforcement	106
5.4.2 Issues with advances in technology	107
4. Changes of regulatory models: from command and control to meta regulation	109
1. Introduction	109
2. The plinth of meta regulation: the “risk management agenda”	110
2.1 The rise of corporate governance	110
2.2 The role of corporate governance in the transformation of risk and risk management: emphasis on process	111
2.3 Governance and the neoliberal logic of risk: responsabilisation and risk taking	112
2.4 Governance and the transformation of organisational activity as risk taking: from risk governance to the risk management agenda (or risk management 2.0): the turning inside out of organisations	113
3. The risk management agenda in practice	114
3.1 Role of internal controls	115
3.1.1 Original meaning of internal controls	115
3.1.2 The transformation of internal controls as risk management: the role of audit and quality control	115
3.2 The risk management agenda’s methodologies	116
3.3 The values of the risk management agenda: responsibility as a “social licence” to operate	117
4. The ISO 31000 Standard as an embodiment of the risk management agenda	119
4.1 Risk management principles	119
4.2 Risk management framework	120
4.3 Risk management process	123
5. Addressing the command and control issues	123
5.1 Command and control shortcomings: lack of expertise and resources	123
5.2 Command and control as responsive regulation: deterrence and compliance	124
6. Smart regulation	125
6.1 Defining smart regulation	125
6.2 Smart regulation and data protection	127
7. From smart regulation to meta regulation	130
7.1 Defining meta regulation	130
8. The role of internal controls and the risk management agenda in collaborative models of regulation	132
8.1 Risk management at the heart of collaborative models of regulation	132
8.2 Summarising the collaborative shifts taking place	133
9. Conclusion: meta regulation and data protection, towards the risk-based approach	135



5. Meta regulation in data protection law: the risk-based approach	136
1. Introduction	136
2. The risk-based approach to data protection: meta regulation with a regulatory focus	137
2.1 Introduction	137
2.2 The regulatory oriented approach's goal: making the regulatory architecture more efficient	138
2.3 Responsibilisation of the data controller through accountability	139
2.3.1 Risk-based approach, responsibility or accountability?	139
2.3.2 History of the accountability principle: the—data protection—principle of accountability: origins	140
2.3.3 The modern accountability principle: responsibility following the risk management agenda	141
2.4 Internal and external responsibility: the value dimension of responsabilisation	145
2.4.1 The alignment of regulatory goals	145
2.4.2 The dual dimension of the risk management agenda's values: democratic ethos and business efficiency, and their recoding as a matter of business goals	148
2.5 The risk-based approach as accountability and, possibly, data protection by design	149
2.6 Accountability, or the risk-based approach? And beyond	150
2.7 Risk-based accountability and the risk-based transformation of the data controller	152
2.8 The risk-based approach as a contradictory implementation of meta regulation?	153
2.9 The scope of the risk-based approach: a focus on safeguards	155
2.10 Summarising the risk-based approach in the GDPR and its rationale	157
2.11 The “regulatory focus” of the risk-based approach in the GDPR, and beyond	160
2.11.1 The GDPR	160
2.11.2 Council of Europe, Convention 108+	160
2.11.3 Canada: PIPEDA and the Privacy Management Program	161
2.11.4 A similar regulatory oriented approach in Canada: Cavoukian's Privacy by Design	162
2.11.5 The Revised OECD Guidelines	162
2.11.6 The APEC Privacy Framework: a more risk-prone risk-based approach?	163
2.12 Beyond the responsabilisation of the regulatees: internal controls, regulatory resources, and enforcement	164
2.12.1 Internal controls: regulatory resource only—or most exclusively—at the internal level	164
2.12.2 The GDPR: a much more collaborative iteration of the risk-based approach	165

2.12.3	The risk-based approach: a piecemeal implementation of the risk management agenda?	168
2.12.4	Enforcement: enforced self-regulation and the ladder of enforcement	170
2.13	Concluding thoughts on the risk-based approach	171
3.	The standard setting oriented risk-based approach	171
3.1	Introduction	171
3.2	The standard setting oriented risk-based approach as a response to regulatory failures	172
3.2.1	Implementation shortcomings	172
3.2.2	Conflicting logic(s): purpose requirement vs purposeless processing, or the conflict between collection based and use based risk assessment	172
3.3	The Microsoft approach	174
3.3.1	A use-based risk-based approach	174
3.3.2	A neoliberal take on risk analysis	175
3.3.3	From a neoliberal take on risk analysis to a deregulatory approach?	176
3.3.4	Concluding remarks on the Microsoft risk-based approach	179
3.4	A new pragmatism: less risky risk and more optimistic approaches	180
3.4.1	Presenting new pragmatisms	180
3.4.2	New pragmatisms and the ideal of natural compliance at the heart of meta regulation	183
6.	Risk and the risk-based approach: Between data protection risks and compliance risks	185
1.	Introduction: various notions of risk at play	185
2.	The ISO's constitutive elements of risk	187
3.	Defining a data protection risk	188
3.1	The computer: the risk source	188
3.2	Risk factors, risks, and harms	189
3.3	Risk factor (1): extent of the processing: increased data quantity	189
3.3.1	Risk from risk factor (1): inaccuracy	190
3.3.2	Harms stemming from inaccuracy	190
3.4	Risk factor (2): properties of the processing: opaque and increased access to, and use of data	190
3.4.1	Risk (1) from risk factor (2): "dragnet effect"	191
3.4.2	Harms stemming from the "dragnet effect"	191
3.4.3	Risk (2) from risk factor (2): loss of control over personal data	191
3.4.4	Harms stemming from loss of control over personal data	191
3.5	Risk factor (3): type of processing: new bureaucratic and managerial practices	193
3.5.1	Risk from risk factor (3): social control	193
3.5.2	Harms stemming from social control	194
3.6	Concluding thoughts on the concept of a data protection risk	195



3.7 The NIST Privacy Engineering and Risk Management in Federal Systems Framework as a risk analysis methodology embodying the notion of data protection risk	196
3.7.1 The notion of data protection risk in the NIST methodology: three feared events	197
4. The notion of risk in the GDPR: compliance risk	198
4.1 Better understanding compliance risk	198
4.2 Traces of the GDPR risk as compliance risk	200
4.3 The risk-based approach as “data protection on the ground”: doing a risk analysis with the CNIL methodology	202
4.4 Other compliance risk management methodologies	206
5. Conclusion: The difference between compliance and “proper” data protection risk, and the logic of meta regulation	208
7. The risk-based approach in practice: Caveats	212
1. Introduction	212
2. Methodological issues	213
2.1 Risk criteria step: taking risks	213
2.2 Different possibilities to assess risks	214
2.2.1 The difference between toxicology and epidemiology	214
2.2.2 Additional caveats surrounding the assessment of risks	218
2.2.3 Examples from DPIA methodologies concerning the different possibilities of assessment	219
2.3 Risk management <i>sensu stricto</i> (ss)	220
2.4 Risk management and data legitimacy	222
3. Regulatory issues	223
3.1 Discretion and consistency: two contradictory requirements	223
3.2 Institutional or secondary risks: competing risks	227
3.3 The risk-based approach and risk-based regulation, or the risk transformation of the regulators themselves	228
4. Risk management on the ground	230
4.1 Adequate collection and use of data	230
4.2 Misplaced pretences at objectivity	231
4.3 Complexity and lack of adequate expertise	233
4.4 The risk-based approach and resource efficiency: a zero-sum game?	234
4.5 Evaluation of efficiency	235
4.6 A new organisational mindset	235
5. Conclusions: meta regulation and utopia	236
Conclusions: Back to the rights/risk-based approaches, and the future of data protection	239
1. Summary of the findings: approaching the debate on rights/risk-based approaches from a different perspective	239
2. The risk-based approach and the future of data protection	248
Bibliography	253
Index	271