

Maximilian von Grafenstein

The Principle of Purpose Limitation in Data Protection Laws

The Risk-based Approach, Principles, and
Private Standards as Elements for Regulating Innovation



Nomos

Schriften zur rechtswissenschaftlichen Innovationsforschung

Herausgeber:

Professor Dr. Wolfgang Hoffmann-Riem

Professor Dr. Karl-Heinz Ladeur

Professor Dr. Hans-Heinrich Trute

Band 12

Maximilian von Grafenstein

The Principle of Purpose Limitation in Data Protection Laws

The Risk-based Approach, Principles, and
Private Standards as Elements for Regulating Innovation



Nomos

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/> or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.



The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at <http://dnb.d-nb.de>

a.t.: Hamburg, Univ., Diss., 2017

ISBN 978-3-8487-4897-6 (Print)
 978-3-8452-9084-3 (ePDF)

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

ISBN 978-3-8487-4897-6 (Print)
 978-3-8452-9084-3 (ePDF)

Library of Congress Cataloging-in-Publication Data

Grafenstein, Maximilian von

The Principle of Purpose Limitation in Data Protection Laws

The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation

Maximilian von Grafenstein

675 p.

Includes bibliographic references and index.

ISBN 978-3-8487-4897-6 (Print)
 978-3-8452-9084-3 (ePDF)

1st Edition 2018

© Nomos Verlagsgesellschaft, Baden-Baden, Germany 2018. Printed and bound in Germany.

This work is subject to copyright. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage or retrieval system, without prior permission in writing from the publishers. Under § 54 of the German Copyright Law where copies are made for other than private use a fee is payable to "Verwertungsgesellschaft Wort", Munich.

No responsibility for loss caused to any individual or organization acting on or refraining from action as a result of the material in this publication can be accepted by Nomos or the author.

To my father

The principle of purpose limitation in data protection law is usually considered as a barrier to data-driven innovation. According to this principle, data controllers must specify the purpose of the collection at the latest when collecting personal data and must not process the data in any way that does not comply with the original purpose. Whether the principle of purpose limitation conflicts with data-driven innovation, however, depends on two sub-questions: On the one hand, one has to know how precisely a data controller must specify the purpose and under which conditions the subsequent processing is fully compatible or incompatible with that purpose. On the other hand, one has to understand the effects of a legal principle such as the principle of purpose limitation on innovation processes. Surprisingly, despite the long-standing and ongoing debate, there is little research that thoroughly examines the regulatory concept of the principle of purpose limitation, and even less its actual impact on innovation. To close this gap, was the aim of this dissertation, which reflects the debate until January 2017.

This dissertation evolved in the context of the interdisciplinary research project “*Innovation and Entrepreneurship*” at the Alexander von Humboldt Institute for Internet and Society. The main research question of this thesis was the result of hands-on observations in our Startup Clinics that we created and carried out for more than four years in order to empirically research the disabling and facilitating factors of internet-enabled innovation. In the Startup *Law* Clinic, where I helped more than 100 startups to cope with the legal challenges they faced during their innovation processes, I realised quite early that most of the startup founders were able to do a great variety of things in a very efficient and creative way, except one: Reliably expect what will happen next month, next week, or even the next day. Under these circumstances of knowledge uncertainty, I wondered how these founders should be able to reliably assess what their future data processing purposes would look like. This hands-on observation served as an inspiring research question and pushed me throughout the four years of its production. The result of this research process was in some way even puzzling to me: As a legal principle, the principle of purpose limitation is not only a highly efficient instrument to protect individuals against the

To my father

risks caused by data-driven innovation but it can even enhance innovation processes of data controllers, when combined with co-regulation instruments.

For the inspiring *tour de force* of these four years, I would like to thank, first and foremost, Prof. Dr. Wolfgang Schulz who not only aroused my interest in regulation as a research discipline but also always immediately and constructively helped me with his oversight, precision in the details and humour. I would also like to especially thank Prof. Dr. Dr. Thomas Schildhauer who has given me the economic perspective on innovation and who in turn has always been pro-actively open to my regulatory viewpoints and ideas. Furthermore, I would like to thank Prof. Dr. Marion Albers, without whose contributions to informational self-determination and data protection my own work would not have been possible, and who compiled the second vote very quickly. Furthermore, I am very thankful and honoured to be included in Prof. Dr. Wolfgang Hoffmann-Riem's, Prof. Dr. Dr. h.c. Karl-Heinz Ladeur's and Prof. Dr. Hans-Heinrich Trute's publication series Legal Research on Innovation ("Rechtswissenschaftliche Innovationsforschung") on that my dissertation is based on. I would also like to thank the German Ministry of the Interior for the financial support of the publication of my thesis.

Finally, I want to thank my colleagues: Elissa Jelowicki, who helped me to revise my thesis throughout the creation process, Jörg Pohle, the "walking library" (I think I do not have to explain that) and all my other colleagues for the endless and inspiring discussions.

Last but not least, I am grateful to my wonderful fiancée Eva Schneider, who in countless evenings of discussions helped me to structure my ideas, and above all motivated me to keep on going.

Content Overview

A. Introduction	31
I. Problem: Conflict between innovation and risk protection	32
1. Innovation as an economic driver for public welfare	32
2. Protection against the risks of innovation	33
3. Uncertainty about the meaning and extent of the principle of purpose limitation	34
4. Practical examples referring to two typical scenarios	35
5. Interim conclusion: Uncertainty about the concept of protection and its legal effects	45
II. Research questions and approach	48
1. Legal research about innovation	48
2. The regulator's perspective	49
3. Possible pitfalls taking the effects of regulation instruments into account	54
III. Course of examination	55
B. Conceptual definitions as a link for regulation	61
I. Innovation and entrepreneurship	61
1. Process of innovative entrepreneurship	63
2. Regulation of innovative entrepreneurship	71
II. Data protection as a risk regulation	79
1. Risk terminology oscillating between “prevention” and “precaution”	79
2. Sociological approaches defining “dangers” and “risks”	82
3. German legal perspectives: Different protection instruments for different types of threat	84
4. Searching for a scale in order to determine the potential impact of data protection risks	89

III. Theories about the value of privacy and data protection	91
1. The individual's autonomy and the private/public dichotomy	91
2. Criticism: From factual to conceptual changes	94
3. Nissenbaum's framework of "contextual integrity"	96
4. Clarifying the relationship between "context" and "purpose"	99
5. Values as a normative scale in order to determine the "contexts" and "purposes"	105
C. The function of the principle of purpose limitation in light of Article 8 ECFR and further fundamental rights	109
I. Constitutional framework	109
1. Interplay and effects of fundamental rights regimes	110
2. The object and concept of protection of the German right to informational self-determination	144
3. Different approach of Article 7 and 8 ECFR with respect to Article 8 ECHR	174
II. The requirement of purpose specification and its legal scale	231
1. Main problem: Precision of purpose specification	231
2. Criticism: Stricter effects on the private than the public sector	295
3. Solution approach: Purpose specification as a risk-discovery process	325
III. Requirement of purpose limitation in light of the range of protection	424
1. Different models of purpose limitation and change of purpose	425
2. Solution approach: Controlling risks that add to those specified previously	483
IV. Data protection instruments in non-linear environments	513
1. Scope of application and responsibility (Article 8 sect. 1 ECFR)	514

2. Legitimacy of processing of personal data (Article 8 sect. 2 ECFR)	547
3. The individual’s “decision-making process” (in light of the GDPR)	563
D. Empirical approach in order to assist answering open legal questions	597
I. Clarifying different risk assessment methodologies	598
1. Different objects of risk assessments	598
2. Different assessment methods	603
3. Interim conclusion: Unfolding complexity	608
II. Multiple-case-studies: Combining research on risks with research on innovation processes	611
1. Reason for the case study approach	611
2. Generalizing the non-representative cases	613
3. Designing the case studies	614
III. Researching the effects of data protection instruments in regards to innovation processes	616
1. Enabling innovation: Contexts, purposes, and specifying standards	616
2. Demonstration on the basis of the examples provided for in the introduction	624
5. Summary: Standardizing “purposes” of data processing	644
E. Final conclusion: The principle of purpose limitation can not only be open towards but also enhancing innovation	649
Bibliography	655

Table of Content

A. Introduction	31
I. Problem: Conflict between innovation and risk protection	32
1. Innovation as an economic driver for public welfare	32
2. Protection against the risks of innovation	33
3. Uncertainty about the meaning and extent of the principle of purpose limitation	34
4. Practical examples referring to two typical scenarios	35
a) Coming from a practical observation: Startups and non-linear innovation processes	36
b) First scenario: Purpose specification by the controller concerning the use of data of its users	37
aa) The unpredictable outcome of entrepreneurial processes	37
bb) Excursus: In which circumstances do data controllers actually need “old” data?	39
c) Second scenario: The limitation of the later use of data collected by third parties	40
aa) No foreseeable negative impact on individuals	40
bb) Negative impact foreseeable on the individuals	42
5. Interim conclusion: Uncertainty about the concept of protection and its legal effects	45
II. Research questions and approach	48
1. Legal research about innovation	48
2. The regulator’s perspective	49
3. Possible pitfalls taking the effects of regulation instruments into account	54
III. Course of examination	55
B. Conceptual definitions as a link for regulation	61
I. Innovation and entrepreneurship	61
1. Process of innovative entrepreneurship	63
a) Key Elements for the entrepreneurial process	63
b) Business Opportunities: Discovery and creation	66

c) Strategic management: Causation and effectuation	69
d) Entrepreneurial contexts: The Law as one influencing factor in innovation processes amongst others	70
2. Regulation of innovative entrepreneurship	71
a) Do laws simply shift societal costs either protecting against or being open to innovation?	72
b) Principles between openness toward innovation and legal uncertainty	73
aa) Legal (un)certainty as a factor that mediates the regulatory burden	74
bb) Conditioning further legal certainty as a promoting factor for entrepreneurial activity	76
c) Interim conclusion with respect to the principle of purpose limitation	77
II. Data protection as a risk regulation	79
1. Risk terminology oscillating between “prevention” and “precaution”	79
2. Sociological approaches defining “dangers” and “risks”	82
3. German legal perspectives: Different protection instruments for different types of threat	84
a) Protection pursuant to the degree of probability	85
b) Protection pursuant to the available knowledge in linear-causal and non-linear environments	87
c) Interim conclusion: Fundamental rights determining the appropriateness of protection	88
4. Searching for a scale in order to determine the potential impact of data protection risks	89
III. Theories about the value of privacy and data protection	91
1. The individual’s autonomy and the private/public dichotomy	91
2. Criticism: From factual to conceptual changes	94
3. Nissenbaum’s framework of “contextual integrity”	96
4. Clarifying the relationship between “context” and “purpose”	99
5. Values as a normative scale in order to determine the “contexts” and “purposes”	105

C. The function of the principle of purpose limitation in light of Article 8 ECFR and further fundamental rights	109
I. Constitutional framework	109
1. Interplay and effects of fundamental rights regimes	110
a) The interplay between European Convention for Human Rights, European Charter of Fundamental Rights and German Basic Rights	111
b) The effects of fundamental rights on the private sector	113
aa) Third-party effect, protection and defensive function	114
(1) European Convention on Human Rights	115
(a) Positive obligations with respect to Article 8 ECHR	116
(b) Right to respect for private life under Article 8 ECHR	117
(2) European Charter of Fundamental Rights	118
(a) Market freedoms and fundamental rights	118
(b) The right to data protection under Article 8 ECFR and/or the right to private life under Article 7 ECFR	120
(3) German Basic Rights	125
(a) Protection function of the right to informational self-determination	126
(b) Priority of contractual agreements and the imbalance of powers	129
(c) Balancing the colliding constitutional positions	130
bb) Balance between defensive and protection function	132
(1) The 3-Step-Test: Assessing the defensive and protection function	133
(2) A first review: decomposing the object and concept of protection	136
(a) Which instruments actually protect which object of protection?	136
(b) Example: “Commercialized” consent threatening the object of protection including...	137
(c) ... individuality?	138

(d) ... solidarity?	139
(e) ... democracy?	140
cc) Equal or equivalent level of protection compared to state data processing?	141
c) Interim conclusion: Interdisciplinary research on the precise object and concept of protection	142
2. The object and concept of protection of the German right to informational self-determination	144
a) Genesis and interplay with co-related basic rights	145
b) Autonomous substantial guarantee	148
c) Right to control disclosure and usage of personal data as protection instrument?	152
d) Infringement by ‘insight into personality’ and ‘particularity of state interest’	158
e) Purpose specification as the essential link for legal evaluation	164
aa) In the public sector: Interplay between the three principles clarity of law, proportionality, and purpose limitation	164
(1) Principles of clarity of law and purpose limitation referring to the moment when data is collected	164
(2) The proportionality test also takes the use of data at a later stage into account	167
bb) In the private sector: The contract as an essential link for legal evaluation	171
f) Interim conclusion: Conceptual link between ‘privacy’ and ‘data processing’	172
3. Different approach of Article 7 and 8 ECFR with respect to Article 8 ECHR	174
a) Genesis and interplay of both rights	175
b) Concept of Article 8 ECHR: Purpose specification as a mechanism for determining the scope of application (i.e. the individual’s ‘reasonable expectation’)	178
aa) Substantial guarantee of “private life”: Trust in confidentiality and unbiased behavior	178
bb) Criteria established for certain cases: Context of collection, nature of data, way of usage, and results obtained	180

cc) Particular reference to the individual's "reasonable expectations"	182
(1) 'Intrusion into privacy'	183
(2) Public situations: 'Systematic or permanent storage' vs. 'passer-by situations'	184
(3) 'Data relating to private or public matters', 'limited use' and/or 'made available to the general public'	186
(4) 'Unexpected use' pursuant to the purpose perceptible by the individual concerned	188
dd) Consent: Are individuals given a choice to avoid the processing altogether?	192
ee) Conclusion: Assessment of 'reasonable expectations' on a case-by-case basis	194
c) Concept of Articles 7 and 8 ECFR: Ambiguous interplay of scopes going beyond Article 8 ECHR	195
aa) Comparing the decisions of the European Court of Justice with the principles developed by the European Court of Human Rights	195
(1) General definition of the term 'personal data' under Article 7 and 8 ECFR instead of case-by-case approach	195
(2) Differences between private life and data protection under Articles 7 and 8 ECFR	198
(a) Protection against first publication and profiles based on public data	198
(b) Protection against collection, storage, and subsequent risk of abuse	201
(3) Reference to further fundamental rights under Article 7 and/or 8 ECFR	205
(a) Which right is used to discuss other fundamental rights?	206
(b) The answer depends on the type of threat posed	207
(4) Protection in (semi)-public spheres irrespective of 'reasonable expectations'?	211
(5) Going beyond the requirement of consent provided for under Article 8 ECHR	214

bb) Interim conclusion: Article 8 ECPR as a regulation instrument?	217
(1) Location of protection instruments under Article 8 ECPR	217
(2) Protection going beyond Article 8 ECHR	218
(3) Remaining uncertainty about the interplay between Article 7 and 8 ECPR	220
cc) Referring to substantial guarantees as method of interpreting fundamental rights in order to avoid a scope of protection that is too broad and/or too vague	222
(1) The reason for why the scope is too vague: Difference between data and information	223
(2) The reason for why the scope is too broad: Increasing digitization in society	225
(3) Advantages and challenges: ‘Personal data’ as legal link for a subjective right	226
(4) Possible consequence: A legal scale provided for by all fundamental rights which determine the regulation instruments under Art. 8 ECPR	229
II. The requirement of purpose specification and its legal scale	231
1. Main problem: Precision of purpose specification	231
a) ECtHR and ECJ: Almost no criteria	232
b) Requirements provided for by European secondary law	234
aa) Central role of purpose specification within the legal system	235
(1) Scope of protection: ‘Personal data’	236
(a) ‘All the means reasonably likely to be used’	236
(b) Example: IP addresses as ‘personal data’?	236
(c) The case of “Breyer vs. Germany”	238
(2) Liability for ‘data processing’: ‘Controller’ and ‘processor’	240
(3) Further legal provisions referring to the purpose	241
bb) Criteria discussed for purpose specification	244
(1) Preliminary note: Clarifying conceptual (mis)understandings	245

(2) Legal opinion on the function of the specification of a purpose	247
(3) Legal opinion on the function of ‘making a specified purpose explicit’	249
(4) Legal opinion on the reconstruction of a purpose and its legitimacy	250
cc) Purposes of processing specified when consent is given	251
dd) Purposes of data processing authorized by legal provisions	252
(1) ePrivacy Directive	252
(2) Data Protection Directive and General Data Protection Regulation	254
(a) Preliminary note: Clarifying conceptual (mis)understandings	255
(b) Legal opinion on ‘performance of a contract’	257
(c) Legal opinion on ‘legal obligation’, ‘vital interests’, and ‘public task’	258
(d) Legal opinion on ‘legitimate interests’	259
c) Transposition of the requirement of purpose specification into German law	262
aa) Purposes of processing authorized by the Telecommunication Law	264
bb) Purposes of processing authorized by the Telemedia Law	266
cc) Purposes of processing authorized by the Federal Data Protection Law	269
(1) Three basic legitimate grounds	269
(2) ‘Performance of a contract’, Article 28 sect. 1 sent. 1 no. 1 BDSG	270
(3) ‘Justified interests of the controller’, Art. 28 sect. 1 sent. 1 no. 2 BDSG	271
(4) ‘Generally accessible data’, Art. 28 sect. 1 sent. 1 no. 3 BDSG	272
(5) Privileges and restrictions pursuant to the purpose	273

dd) Purposes of processing specified when consent is given	275
(1) Not a waiver but execution of right to informational self-determination	276
(2) Requirements for consent and consequences of its failure	277
(3) Discussion on the degree of precision of a specified purpose	278
ee) Comparison with principles developed by the German Constitutional Court	281
(1) Public sector: Purpose specification as a result of the principle of clarity of law	281
(a) Function of purpose specification (basic conditions)	281
(b) Examples for specific purposes: Certain areas of life or explicitly listed crimes	284
(c) Examples for unspecific purposes: Abstract dangers or unknown purposes	286
(d) Liberalization of the strict requirement by referring to the object of protection	290
(2) Private sector: 'Self-control of legitimacy'	293
2. Criticism: Stricter effects on the private than the public sector	295
a) Difference in precision of purposes specified by legislator and data controllers	296
aa) Data processing for undisputed 'marketing purposes' authorized by law	297
bb) Disputed 'marketing purposes' specified by data controllers	298
cc) Further examples for different scales applied in order to specify the purpose	299
dd) Can the context help interpret a specified purpose?	300
ee) A different scale for 'purpose specification' pursuant to the German concept of protection	301
ff) Interim conclusion: Do regulation instruments dictate the scale for 'purpose specification'?	303

b) Further ambiguities and possible reasons behind the same	304
aa) Common understanding about the function of ‘purpose specification’	305
bb) Ambiguous understanding regarding the functions of ‘making specified purpose explicit’	306
cc) Arguable focus on data collection for legal evaluation in the private sector	307
dd) Arguable legal consequences surrounding the validity of the consent	310
c) The lack of a legal scale for ‘purpose specification’ in the private sector	312
aa) No legal system providing for ‘objectives’ of data processing in the private sector	313
bb) Differentiating between the terms ‘purpose’, ‘means’ and ‘interest’	315
(1) ‘Interests’ protected by the controller’s fundamental rights	316
(2) Is the ‘purpose’ determined by the individual’s fundamental rights?	318
bb) Inclusion or exclusion of future ‘purposes’ and ‘interests’	320
(1) Present interests vs. future interests	321
(2) Purpose specification pursuant to the type of threat?	323
d) Summary of conceptual ambiguities	324
3. Solution approach: Purpose specification as a risk-discovery process	325
a) Regulative aim: Data protection for the individual’s autonomy	327
aa) Intermediate function of data protection	328
(1) Different functions of rights (opacity and transparency)	329
(2) Disconnecting the exclusive link between data protection to privacy	331
(3) Data protection for all rights to privacy, freedom, and equality	334

bb) Purpose specification as a risk regulation instrument	336
(1) ‘A risk to a right’: Quantitative vs. qualitative evaluation?	337
(a) Challenges of bridging risks to rights	338
(b) Example: German White Paper on DPIA	339
(c) Criticism: Incoherence of current risk criteria	341
(2) Purpose specification discovering risks posed to all fundamental rights	343
(a) Pooling different actions together in order to create meaning	343
(b) Separating unspecific from specific risks (first reason why data protection is indispensable)	345
(c) Central function with respect to all fundamental rights (second reason why data protection is indispensable of data protection)	348
(3) Function of making specified purposes explicit	350
cc) Interim conclusion: Refining the concept of protection	353
(1) Tying into the Courts’ decisions and European legislation	353
(2) Advantages compared to existing (unclear) concepts of protection	356
(a) Effectiveness and efficiency of protection instruments	356
(b) Appropriate concept for innovation processes	357
(c) Excursus: Objective vs. subjective risks	359
b) Fundamental rights which determine purpose requirements	361
aa) Right to privacy (aka ‘being left alone’)	361
(1) Unfolding specific guarantees of privacy	362
(a) At home: Protection of ‘haven of retreat’	363
(b) Using communications: Protection against ‘filtering opinions’	365

(c) “Privacy in (semi)-public spheres”: Protection against the risks of later usage of data	366
(2) Necessity requirement, irrespective of inconvenience	370
(3) ‘Framing’ privacy expectations	371
(a) Research on the individual’s decision making process (consent)	372
(b) First example: The legislature’s considerations on the use of ‘cookies’	374
(c) Second example: Considerations surrounding ‘unsolicited communications’	375
bb) Right to self-determination in public	377
(1) Clarification of substantial guarantees	377
(2) First publication: Strict requirements	378
(a) Necessity of publication	379
(b) Strict requirements for consent	380
(3) Re-publication: Weighing ‘interests’ against ‘old and new purposes’	382
(a) Misconceptions in the decision of “Mr. González vs. Google Spain”	383
(b) Excursus: Case law provided for by the German Constitutional Court	385
(c) Conclusion in regards to the decision of “Mr. González vs. Google Spain”	387
cc) Internal freedom of development	389
(1) Does the German right to informational self- determination provide for such a guarantee?	389
(2) Discussion on such a substantial guarantee	392
(3) Articles 7 and/or 8 ECFR: Information pursuant to insights into personality and possibilities of manipulation	394

dd) Specific rights to freedom	397
(1) Focus on the collection of data: Omission by the individual of exercising their rights out of fear	398
(a) Considerations of the Courts with respect to the freedom of expression and the individuals risk of being unreasonably suspected by the State	398
(b) Considerations on further rights of freedom	400
(2) Focus on the later usage of data or information: Restriction or hindrance of exercise of rights of freedom through usage of data or information	403
(3) Interim conclusion: How “privacy in public” can be further determined	404
(a) Specific contexts of collection of personal data	405
(b) Later use of personal data in the same context	407
(c) Protection instruments enabling the individual to adapt to or protect him or herself against the informational measure	411
ee) Rights to equality and non-discrimination	417
(1) In the public sector: Criteria for intensity of infringement	417
(2) In the private sector: ‘Tool of opacity’ vs. private autonomy?	418
(3) Interim conclusion: Additional legitimacy requirement for the data-based decision-making process	420
c) Conclusion: Purpose specification during innovation processes	422

III. Requirement of purpose limitation in light of the range of protection	424
1. Different models of purpose limitation and change of purpose	425
a) European models: ‘Reasonable expectations’ and purpose compatibility	425
aa) Change of purpose pursuant to ECtHR and ECJ	426
(1) ECtHR: ‘Reasonable expectations’ as a main criteria	426
(2) ECJ: Reference to data protection instruments instead of ‘reasonable expectations’	428
(a) Are the terms ‘necessity’, ‘adequacy’ and ‘relevance’ used as objective criteria for the compatibility assessment?	429
(b) Purpose identity for the consent	430
bb) Compatibility assessment required by the Data Protection Directive with respect to the opinion of the Art. 29 Data Protection Working Party	431
(1) Preliminary analysis: Pre-conditions and consequences	432
(2) Example: The expectations of a customer purchasing a vegetable box online	435
(3) Criteria for the substantive compatibility assessment	436
(a) First criteria: ‘Distance between purposes’	436
(b) Second criteria: ‘Context and reasonable expectations’	437
(c) Third criteria: ‘Nature of data and impact on data subjects’	439
(d) Fourth criteria: ‘Safeguards ensuring fairness and preventing undue impact’	441
(4) Excursus: Compatibility of ‘historical, statistical or scientific purposes’	444
(a) Specification of the compatibility assessment (even prohibiting positive effects)	444
(b) Safeguards corresponding to the characteristics of the purposes	445

(c) Hierarchy of safeguards: From anonymization to functional separation	446
cc) Purpose identity required by the ePrivacy Directive	447
(1) Strict purpose identity for the processing of ‘communication data’, ‘traffic data’ and ‘location data other than traffic data’	447
(2) The individual’s consent as an exclusive legal basis for a change of purpose	448
dd) Interim conclusion: A lack in the legal scale for compatibility assessment	449
b) German model: Purpose identity and proportionate change of purpose	452
aa) Change of purpose in the private sector pursuant to ordinary law	453
(1) Strict purpose identity required by Telemedia Law and Telecommunication Law	453
(2) The more nuanced approach established by the Federal Data Protection Law	454
bb) Comparison with the principles developed by the German Constitutional Court for the public sector	457
(1) Strict requirement of purpose identity limiting the intensity of the infringement	458
(2) Proportionate change of purpose	461
(3) Identification marks as a control-enhancing mechanism	466
cc) Alternative concepts provided for in German legal literature	467
(1) Purpose identity and informational separation of powers	468
(a) Purpose specification by the individual instead of the controller	469
(b) Principle of purpose limitation and informational separation of powers	470
(c) Example of re-registration: Collection and transfer of data on the citizen’s request	472
(2) Compatibility of purposes	473
(a) Criticism of the “subjective” purpose approach	473

(b) Compatibility instead of identity of purposes	474
(c) Supplementing protection instruments	475
(3) Purpose identity and change of purpose as ‘a threshold for duty of control’	476
(a) Criticism of purpose compatibility	477
(b) Specification, identity and change of purpose as equivalent regulation instruments	477
(c) The opposing fundamental rights providing for the objective legal scale	478
dd) Interim conclusion: Right to control data causing a ‘flood of regulation’	479
2. Solution approach: Controlling risks that add to those specified previously	483
a) Conceptual shift: From the exclusion of unspecific risks to the control of specific risks	483
aa) Different types of changes of purpose in light of different types of risks	484
(1) Purpose compatibility as an “umbrella assessment”	484
(2) Custer’s and Ursic’s taxonomy: “Data recycling, repurposing, and recontextualization”	486
(3) Clarification of an objective scale: “Same risk, higher risk, and another risk”	489
bb) Refinement of current concepts of protection	490
(1) Article 8 ECPR and European secondary law	490
(a) “Purpose identity” forbidding additional risks (than specified before)	491
(b) Further protection instruments that can avoid purpose incompatibility	491
(c) Systemizing the criteria for the compatibility assessment	493
(2) Right to private life under Article 8 ECHR and the right to informational self-determination	496
cc) Applying a ‘non-linear perspective’	497

b) Substantial guarantees: Providing criteria for a compatibility assessment	499
aa) Right of ‘being left alone’: ‘Reasonable expectations’ determined by risks	500
bb) Self-representation in the public: A balancing exercise instead of purpose determination	503
cc) Internal freedom of development: Specific instead of preliminary information	505
dd) External freedoms of behavior: Purpose identity as one potential element amongst several protection instruments	507
ee) Equality and non-discrimination: Specifying incompatible purposes in the course of social life	508
c) Conclusion: Purpose limitation in decentralized data networks	510
IV. Data protection instruments in non-linear environments	513
1. Scope of application and responsibility (Article 8 sect. 1 ECFR)	514
a) Problems in practice: A balance between too much and too little protection	515
aa) How data may be related to an individual	515
bb) Anonymization of personal data	518
cc) Again: The problem of a “yes-or-no-protection” solution	521
b) Alternative solution: Scope(s) pursuant to the type of risk	522
aa) Theoretical starting point: Different levels of protection	523
(1) Pro and cons for precautionary protection against abstract dangers	524
(2) Abstract precautionary protection only in cases of special danger	525
(3) Advantages of a nuanced approach	527
bb) Differentiating between the general scope of protection and the application of specific protection instruments	530
(1) General scope of protection enabling specification of purpose (aka risk)	531

(2) Application of protection instruments determined by specific risks	532
(a) Rights to privacy	533
(b) Right of self-representation in the public	534
(c) Internal freedom of behavior	535
(d) Rights to freedom and non-discrimination	538
(3) Again: General scope of protection requiring data security (against unspecific risks)	539
c) Excursus: Responsibility (“controller” and “processor”)	542
(1) Cumulative responsibility for precautionary protection	544
(2) Cooperative responsibility for preventative protection	545
2. Legitimacy of processing of personal data (Article 8 sect. 2 ECFR)	547
a) Same measures but differently applied in the public and private sector	548
aa) Different risks in the public and private sector	549
bb) Example: Requirements to specify the purpose and limit the processing at a later stage	552
cc) Legal-technical constraints surrounding the prohibition rule	553
b) Possible approaches of regulation in the private sector	554
aa) Classic instruments: Specific legal provisions, broad legal provisions, and/or consent	555
bb) Conceptual shift: From a legal basis to ‘legitimacy assessment’	556
cc) Side note: State regulated self-regulation increasing legal certainty	558
dd) Interplay of consent and legal provisions	560
c) Interim conclusion: Balancing the colliding fundamental rights	562
3. The individual’s “decision-making process” (in light of the GDPR)	563
a) Static perspective: Opt-in or opt-out procedure for consent?	565
aa) Classic discussion regarding current data protection laws	565

bb) Further approaches considered by the legislator and Constitutional Courts	567
cc) Requirements illustrated so far, with respect to different guarantees	569
b) Dynamic perspective: Interplay of several protection instruments	570
aa) Consent: “Later processing covered by specified purpose?”	570
(1) Risks as object of consent (not data)	572
(2) Extent of consent limiting the later use of data (instead of being illegal as a whole)	574
(3) Change of purpose: Opt-out procedures for higher and opt-in procedures for other risk	577
bb) Clarifying recital 50 GDPR: “Separate legal basis if purpose not compatible”	579
(1) Arg. ex contrario: Is an incompatible purpose legal on a separate legal basis?	580
(2) Differentiating between “not compatible” and “incompatible” purposes	581
(3) Assessment of safeguards that ensure that purposes do not (definitely) become incompatible	581
cc) Legal basis and opt-out: Change of purpose	582
(1) Opt-out: A risk-reducing protection instrument	583
(2) Examples: New risks not covered by consent (in light of the specified purpose)	584
(3) Examples: New risks not covered by a former applicable provision	585
dd) Information duties and further participation rights	586
(1) Controller’s duties of information	587
(a) Data collection: Customizing information in relation to daily decision-making processes	588
(b) Change of purpose: Interpreting information duties regarding specific risks	589
(c) Profiling and automated decision-making	589
(2) Individual’s right to rectification	592
c) Conclusion: Specifying the decision-making process (Art. 24 and 25 GDPR)	592

D. Empirical approach in order to assist answering open legal questions	597
I. Clarifying different risk assessment methodologies	598
1. Different objects of risk assessments	598
a) Risk-based approach of purpose specification and limitation (Art. 5 sect. 1 lit. b GDPR)	598
b) Data Protection Impact Assessment (Art. 35 GDPR)	599
c) Further methodologies (technology assessment and surveillance impact assessment)	601
2. Different assessment methods	603
a) Examining abstract constitutional positions from a social science perspective	604
b) Pre-structuring interests through multiple-stakeholder and expert participation	605
c) Specifying ‘decision-making process’ by user-centered development of data protection-by-design	605
3. Interim conclusion: Unfolding complexity	608
II. Multiple-case-studies: Combining research on risks with research on innovation processes	611
1. Reason for the case study approach	611
2. Generalizing the non-representative cases	613
3. Designing the case studies	614
III. Researching the effects of data protection instruments in regards to innovation processes	616
1. Enabling innovation: Contexts, purposes, and specifying standards	616
a) Enabling data controllers to increase legal certainty	617
b) Enhancing competition on the “data protection” market	617
c) Remaining questions in relation to the effects of legal standards	620
2. Demonstration on the basis of the examples provided for in the introduction	624
a) Example of “personalized advertising”	624
aa) Preliminary legal analysis	624
(1) Initial product and business model: Internal freedom of development	625
(2) Change of product and business model: No substantive change of purpose	626

bb) Open legal questions ('propositions')	627
(1) Standardization of "personalized marketing" purpose	628
(2) Competitive advantage	629
b) Example of "anonymized data for statistic/research purposes"	630
aa) Preliminary legal analysis	630
(1) Processing of public personal data: Self-determination in public	630
(2) The taxi driver: Attributing anonymized data to passengers	631
bb) Open legal questions ('propositions')	633
(1) Standardization of "statistical" or "scientific" purposes	633
(2) Competitive advantage	635
c) Example of "scoring in the employment context"	636
aa) Preliminary legal analysis	636
(1) Re-publication of personal data: fair balance instead of a priority rule	637
(2) Freedom to find an occupation: Participation instruments	639
bb) Open legal questions ('propositions')	642
(1) Standardization of "profiling potential employees"	642
(2) Signaling legal certainty (to the "workers' council")	643
5. Summary: Standardizing "purposes" of data processing	644
E. Final conclusion: The principle of purpose limitation can not only be open towards but also enhancing innovation	649
Bibliography	655