

Personal Data Protection Law

Kişisel Verilerin Korunması Hukuku

Murat Volkan Dülger, Gülçin Gümüş

4th ed., Seçkin Publishing, Ankara, February 2026, 752 pages, ISBN 9786253817138

■ Table of contents

Preface to the Fourth Edition	6
Preface to the Third Edition	7
Preface to the Second Edition	9
Preface to the First Edition	11
Abbreviations	31

CHAPTER ONE

THE CONCEPT OF PERSONAL DATA AND THE PROTECTION OF PERSONAL DATA AS A RIGHT

§ 1. THE CONCEPT OF PERSONAL DATA	33
I. DEFINITION OF PERSONAL DATA	33
II. SCOPE AND ELEMENTS OF PERSONAL DATA	37
A. In General	37
B. Elements of Personal Data	38
1. Existence of a Piece of Data	38
2. The Data Rendering the Person Identified or Identifiable	43
a. Direct Identifiers	44
b. Indirect Identifiers	44
c. Limits of Identifiability	49
d. The Status of Anonymised Data	50
e. The Status of Pseudonymised (Aliased / Masked / Redacted) Data	51
f. The Status of Encrypted or Partially Redacted Data	53
3. The Data Relating to a Person	53
4. The Data Belonging to a Natural Person	56
C. Data Giving Rise to Doubt as to Whether They Are Personal Data	60
1. In General	60
2. The Status of Unclassified Physical Data	61
III. SPECIAL CATEGORIES OF (SENSITIVE) PERSONAL DATA	62
§ 2. EMERGENCE OF THE RIGHT TO THE PROTECTION OF PERSONAL DATA	64
I. IN GENERAL	64
II. PERSONAL DATA AND THE SURVEILLANCE SOCIETY	65
A. Surveillance in Modern Society	66
1. The Conception of Surveillance of Karl Marx, Max Weber and George Orwell	69
2. Michel Foucault's Conception of Surveillance	72
B. Electronic Surveillance Emerging as a Result of Technological Developments	74
III. NATURE OF THE RIGHT TO THE PROTECTION OF PERSONAL DATA	74
A. In General	74
B. Legal Nature of the Right to the Protection of Personal Data	75

1.	The View That It Is an Economic Right	76
a.	The View That It Is a Property Right	76
b.	The View That It Is an Intellectual Property Right	78
2.	The View That It Is a Human Right	78
C.	The Debate on Whether It Is an Independent Right	79
1.	The View That Considers It under the Right to Respect for Private Life	79
2.	The View That It Is an Independent Right	80
3.	Our View	81
§ 3.	PROTECTION OF PERSONAL DATA IN THE FUNDAMENTAL INSTRUMENTS	85
I.	PROTECTION OF PERSONAL DATA IN INTERNATIONAL INSTRUMENTS	85
A.	OECD (Organisation for Economic Co-operation and Development)	85
B.	United Nations	87
1.	Universal Declaration of Human Rights	87
2.	United Nations International Covenant on Civil and Political Rights (ICCPR)	87
3.	UN Guidelines for the Regulation of Computerized Personal Data Files	89
C.	Council of Europe	89
1.	Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data	90
2.	Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows (Protocol on Transborder Data Flows)	92
3.	European Convention on Human Rights	93
D.	The European Union	94
1.	Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (Data Protection Directive)	95
2.	Charter of Fundamental Rights of the European Union	99
3.	Directive 2002/58/EC of the European Parliament and of the Council concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (ePrivacy Directive)	100
4.	Directive 2016/680 on the Protection of Personal Data in Law Enforcement and Criminal Proceedings (Law Enforcement Directive – LED)	100
5.	Regulation (EU) 2018/1725 on Data Protection by the Institutions of the European Union	102
6.	European Union General Data Protection Regulation 2016/679 (GDPR)	102
II.	PROTECTION OF PERSONAL DATA IN NATIONAL LEGISLATION	110
A.	The 1982 Constitution	110
B.	Law on the Protection of Personal Data	112
C.	Turkish Criminal Code	113
§ 4.	PROTECTION OF PERSONAL DATA AS A HUMAN RIGHT	113
I.	THE CONCEPT OF A HUMAN RIGHT	113
II.	THE PLACE OF THE RIGHT TO THE PROTECTION OF PERSONAL DATA AMONG HUMAN RIGHTS	116
III.	THE RIGHT TO THE PROTECTION OF PERSONAL DATA IN THE JUDGMENTS OF THE EUROPEAN COURT OF HUMAN RIGHTS	118
A.	Scope of the Concept of Private Life Referred to in Article 8 of the Convention	119
B.	The Requirement That Interference with the Right to the Protection of Personal Data Be Based on a Statutory Provision	130
C.	Unlawful Storage, Use and Disclosure of Personal Data	134
D.	The Requirement That Interferences with the Right to the Protection of Personal Data Be Limited to a Legitimate Aim	135

IV.	THE RIGHT TO THE PROTECTION OF PERSONAL DATA IN THE JUDGMENTS OF THE CONSTITUTIONAL COURT	139
A.	Scope of the Concept of Private Life Referred to in Article 20 of the Constitution	139
B.	The Right to the Protection of Personal Data Protected by Paragraph 3 of Article 20 of the Constitution and Its Scope	142
C.	The Requirement That the Right to the Protection of Personal Data Be Regulated by Law	144
V.	ASSESSMENT AND OUR VIEW	146

CHAPTER TWO

SCOPE AND CONTENT OF THE LAW, BASIC CONCEPTS AND PRINCIPLES

§ 5.	THE NEED TO PROTECT PERSONAL DATA THROUGH A BASIC PIECE OF LEGISLATION, AND THE DEVELOPMENT AND EMERGENCE OF THE LEGISLATION	151
I.	THE NEED TO PROTECT PERSONAL DATA THROUGH LEGISLATION	151
II.	DEVELOPMENT AND EMERGENCE OF THE LEGISLATION	161
§ 6.	THE DATA PROTECTION SYSTEM PROVIDED FOR BY THE LAW	164
I.	IN GENERAL	164
II.	SCOPE AND STRUCTURE OF THE LAW ON THE PROTECTION OF PERSONAL DATA (KVKK)	167
A.	Purpose	167
B.	Scope	169
1.	Cases Falling within the Scope of the Law	169
a.	Natural Persons Whose Personal Data Are Processed	169
b.	Natural and Legal Persons Who Process Personal Data	170
c.	Processing of Personal Data Wholly or Partly by Automated Means or, Provided That It Forms Part of a Data Filing System, by Non-Automated Means	170
2.	Cases Falling outside the Scope	172
a.	Cases Wholly Excluded from the Scope of the Law	172
i.	Processing of Personal Data by Natural Persons in the Course of Activities Relating Exclusively to Themselves or to Family Members Living in the Same Dwelling, Provided That the Data Are Not Disclosed to Third Parties and the Obligations Relating to Data Security Are Complied With	172
ii.	Processing of Personal Data for Official Statistics and, by Being Anonymised, for Purposes Such as Research, Planning and Statistics	174
iii.	Processing of Personal Data for Artistic, Historical, Literary or Scientific Purposes or within the Scope of Freedom of Expression	175
iv.	Processing of Personal Data within the Scope of Preventive, Protective and Intelligence Activities Carried Out by Public Institutions and Organisations Assigned Duties and Powers by Law to Safeguard National Defence, National Security, Public Security, Public Order or Economic Security	177
v.	Processing of Personal Data by Judicial Authorities or Execution Authorities in Connection with Investigation, Prosecution, Trial or Execution Proceedings	179
b.	Cases Partly Excluded from the Scope of the Law	181
i.	In General	181
ii.	Where the Processing of Personal Data Is Necessary for the Prevention of Offences or for a Criminal Investigation	182
iii.	Processing of Personal Data Made Public by the Data Subject Himself or Herself	183
iv.	Where the Processing of Personal Data Is Necessary for the Performance of Supervisory or Regulatory Duties and for Disciplinary Investigation or Prosecution by Competent and Authorised Public Institutions and Organisations and by Professional Organisations with the Status of Public Institutions, on the Basis of Authority Conferred by Law	184

v.	Where the Processing of Personal Data Is Necessary for the Protection of the Economic and Financial Interests of the State in Budgetary, Tax and Fiscal Matters	184
C.	Basic Principles Relating to the Processing of Personal Data in the KVKK	184
III.	THE SUPERVISORY MECHANISM PROVIDED FOR IN THE KVKK	186
IV.	THE PERSONAL DATA PROTECTION AUTHORITY, ITS ORGANISATIONAL STRUCTURE AND DUTIES	189
A.	In General	189
B.	The Personal Data Protection Board and Its Duties	190
C.	The Presidency	192
V.	RELEVANT REGULATIONS	192
VI.	DECISIONS OF THE BOARD	193
§ 7.	BASIC CONCEPTS RELATING TO THE PROTECTION OF PERSONAL DATA	195
I.	IN GENERAL	195
II.	BASIC CONCEPTS	195
A.	Processing of Personal Data	195
B.	Data Filing System	197
C.	Data Subject	200
D.	Controller	201
E.	Joint Controller	210
1.	The Concept	210
2.	The Place of the Joint Controller in the KVKK and the GDPR	211
3.	Judgment of the Court of Justice of the European Union (CJEU) of 5 June 2018 in Wirtschaftsakademie and Facebook Ireland	216
4.	Judgment of the CJEU of 10 July 2018 in Jehovah's Witnesses	219
5.	Judgment of the CJEU of 29 July 2019 in Fashion ID and Facebook Ireland	222
F.	Processor	224
1.	In General	224
2.	The Processor in the GDPR	230
a.	Obligations of the Processor	230
b.	The Contract to Be Concluded between the Processor and the Controller	232
G.	Explicit Consent	234
H.	Transfer of Personal Data	238
I.	Data Controllers' Registry	239
i.	Personal Data Breach	240
J.	Erasure, Destruction or Anonymisation of Personal Data	243
§ 8.	PRINCIPLES OF DATA PROTECTION LAW	245
I.	IN GENERAL	245
II.	BASIC PRINCIPLES RELATING TO THE PROCESSING OF PERSONAL DATA	246
A.	Fairness and Compliance with the Rule of Good Faith	247
1.	Compliance with the Law and the Rules of Good Faith under the KVKK	247
2.	Lawfulness, Fairness and Transparency under the GDPR	255
B.	Processing for Specified, Explicit and Legitimate Purposes	258
1.	Collection of Data for Specified, Explicit and Legitimate Purposes	259
a.	The Purpose Being Specified and Explicit	259
b.	The Purpose Being Legitimate	262
2.	Processing of Data in Accordance with the Purposes Specified for Their Collection	265
C.	Data Being Relevant, Limited and Proportionate to the Purpose for Which They Are Processed	268
1.	Personal Data Must Be Relevant to the Purpose of Processing	270

2.	Purpose Limitation	270
3.	The Amount of Data Must Be Limited/Proportionate to What Is Necessary for the Purpose Determined by the Controller	271
a.	Importance and Understanding of the Principle	271
b.	Other Points to Be Noted with a View to Compliance with the Principle	280
D.	Being Accurate and, Where Necessary, Kept up to Date	281
1.	In General	281
2.	The Status of Inaccurately Processed Data	285
3.	When Data Must Be Kept up to Date	286
4.	Responsibilities of the Controller and the Data Subject in Obtaining Up-to-Date Information	286
E.	Retention of Data for the Period Necessary for the Purpose	290
1.	In General	290
2.	Cases in Which Personal Data Have Become Unnecessary or Purposeless for the Intended Purpose	291
3.	The Period Determined by the Controller for the Purpose of Data Processing	292
4.	Choosing One of the Methods of Erasure, Destruction or Anonymisation in Order to Eliminate Personal Data That Have Become Unnecessary or Purposeless for the Intended Purpose	293
F.	Integrity and Confidentiality	295
G.	The Accountability Requirement	296
H.	Data Protection by Design and by Default	298

CHAPTER THREE

RULES ON DATA PROCESSING IN PERSONAL DATA PROTECTION LAW

§ 9.	CONDITIONS FOR THE PROCESSING OF PERSONAL DATA	301
I.	IN GENERAL	301
II.	PROCESSING OF PERSONAL DATA	302
A.	Conditions for the Processing of Personal Data Other than Special Categories	304
1.	Explicit Consent of the Data Subject	306
a.	Conditions of Explicit Consent	307
i.	Relating to a Specific Matter	307
ii.	Being Informed	309
iii.	Being Expressed of One's Own Free Will	311
b.	Additional Conditions Relating to Consent in the GDPR	313
c.	The Problem of Consent in the Processing of Children's Personal Data	315
i.	In General	315
ii.	Consent of the Holder of Parental Responsibility	316
iii.	The Requirement That Consent Be Informed	317
iv.	The Approach of the Personal Data Protection Authority	317
d.	Controversial Points Relating to Explicit Consent	318
i.	Comparison of Explicit Consent and the Statutory Conditions for the Processing of Personal Data	318
ii.	Obtaining Explicit Consent despite the Existence of the Processing Conditions Listed in the Law	318
iii.	Whether Explicit Consent May Be Made Subject to a Condition	320
iv.	Providing Additional Advantages in Return for Consent When Obtaining Explicit Consent	323

v.	The Manner of Obtaining Explicit Consent	326
vi.	Whether Explicit Consent May Be Withdrawn	328
vii.	Validity of Data Obtained with Lawful Consent before the Date of Entry into Force of the KVKK	329
2.	Being Expressly Provided for in Laws	332
3.	Where It Is Necessary for the Protection of the Life or Physical Integrity of a Person Who Is Unable to Express Consent Owing to Actual Impossibility or Whose Consent Is Not Recognised as Legally Valid, or of Another Person	335
4.	Where the Processing of Personal Data of the Parties to a Contract Is Necessary, Provided That It Is Directly Related to the Conclusion or Performance of the Contract	337
5.	Where It Is Necessary for the Controller to Fulfil Its Legal Obligation	343
6.	Where the Data Have Been Made Public by the Data Subject Himself or Herself	346
7.	Where Data Processing Is Necessary for the Establishment, Exercise or Protection of a Right	355
8.	Where Data Processing Is Necessary for the Legitimate Interests of the Controller, Provided That the Fundamental Rights and Freedoms of the Data Subject Are Not Harmed	357
B.	Conditions for the Processing of Special Categories of Personal Data	362
1.	In General	362
2.	Certain Debates Concerning the Scope of Special Categories of Personal Data	363
2.	Explicit Consent	369
3.	Being Expressly Provided for in Laws	370
4.	Where It Is Necessary for the Protection of the Life and Physical Integrity of a Person Who Is Unable to Express Consent Owing to Actual Impossibility or Whose Consent Is Not Recognised as Legally Valid, or of Another Person	371
5.	In the Case of Personal Data Made Public by the Data Subject, Conformity with the Data Subject's Intention in Making Them Public	371
6.	Where It Is Necessary for the Establishment, Exercise or Protection of a Right	373
7.	Where It Is Necessary for the Purposes of Protecting Public Health, Preventive Medicine, Medical Diagnosis, the Provision of Treatment and Care Services, and the Planning, Management and Financing of Health Services, by Persons under an Obligation of Secrecy or by Authorised Institutions and Organisations	373
8.	Where It Is Necessary for the Fulfilment of Legal Obligations in the Fields of Employment, Occupational Health and Safety, Social Security, Social Services and Social Assistance	374
9.	Where Processing by Foundations, Associations and Other Non-Profit Organisations or Bodies Established for Political, Philosophical, Religious or Trade-Union Purposes Concerns Their Current or Former Members and Affiliates or Persons in Regular Contact with Such Organisations and Bodies, Provided That It Complies with the Legislation to Which They Are Subject and with Their Purposes, Is Limited to Their Fields of Activity and the Data Are Not Disclosed to Third Parties	375
III.	TRANSFER OF PERSONAL DATA	376
A.	Transfer of Personal Data within the Country	376
B.	Transfer of Personal Data Abroad	382
1.	In General	382
2.	Cases Deemed to Be Transfer Abroad	383
a.	Transfer of Personal Data to a Foreign Country	384
b.	The Status of Cloud Services	384
c.	Transfer to a Company Whose Servers Are Located Abroad	386
3.	Conditions for Transfer Abroad	386
a.	Transfer of Data Abroad Where an Adequacy Decision Exists	388
b.	Transfer of Data Abroad in the Absence of an Adequacy Decision	391

i.	Existence of an Agreement Not Having the Nature of an International Treaty	392
ii.	Signing of a Standard Contract	394
iii.	Binding Corporate Rules	397
iv.	Signing of a Written Undertaking	398
c.	Exceptional Transfer of Data Abroad Where There Is No Adequacy Decision and Appropriate Safeguards Cannot Be Provided Either	398
4.	Steps to Be Taken in Order by Controllers When Transferring Data Abroad	400
§ 10.	RIGHTS OF THE DATA SUBJECT	402
I.	IN GENERAL	402
II.	RIGHTS OF THE DATA SUBJECT	403
A.	Transparent Information to the Data Subject on the Exercise of His or Her Rights	403
B.	The Data Subject's Right of Access	407
1.	Nature and Purpose of the Right	407
2.	Scope	409
C.	Data Portability	415
D.	Right to Rectification	418
E.	Right to Object	419
F.	Right to Erasure/Right to Be Forgotten	422
1.	The Process by Which the Right Emerged	424
2.	Scope	433
a.	Where the Personal Data Are No Longer Necessary in Relation to the Purposes for Which They Were Collected or Processed	435
b.	Where the Data Subject Objects to the Processing and There Are No Overriding Legitimate Grounds for the Processing	436
c.	Where the Personal Data Have Been Unlawfully Processed	437
d.	Where the Personal Data Must Be Erased in Order to Comply with a Legal Obligation to Which the Controller Is Subject	437
e.	Where the Personal Data Concerned Were Collected in Connection with the Provision on Online Services Offered to Children	439
G.	Right to Restriction of Processing	440
H.	Right to Request That Third Parties Be Notified of the Operations	441
I.	Right to Restrict Automated Decision-Making	442
i.	Right to Claim Compensation for Damage	445
III.	MATTERS TO BE OBSERVED IN GIVING EFFECT TO THE RIGHTS OF THE DATA SUBJECT	445
A.	As Regards the Procedure for Exercising the Rights	445
B.	As Regards Time Limits	449
C.	Fee	453
D.	Verifying the Identity of the Persons Making a Request	455
E.	Method to Be Used in Responding	456
IV.	EXCEPTIONS	459
§ 11.	OBLIGATIONS OF THE CONTROLLER AND THE PROCESSOR	460
I.	OBLIGATIONS OF THE CONTROLLER	460
A.	Obligation to Inform	460
1.	In General	460
2.	Procedures and Principles to Be Followed in Fulfilling the Obligation to Inform	461
a.	Scope of the Obligation to Inform	461
b.	Procedures and Principles Relating to the Obligation to Inform	462

c.	The Obligation to Inform Where the Personal Data Are Not Obtained from the Data Subject	471
B.	Obligation to Enable the Data Subject to Exercise His or Her Rights	472
C.	Obligations Relating to Data Security	472
1.	In General	472
2.	Decisions of the Board Relating to Data Security	477
a.	Adequate Measures to Be Taken in Respect of Special Categories of Personal Data	477
i.	Measures Relating to the Policy and Procedure for the Protection, Storage and Processing of Personal Data	477
ii.	Measures Relating to Employees Involved in the Processing of Special Categories of Personal Data	478
iii.	Where the Environments in Which Special Categories of Personal Data Are Processed, Stored and/or Accessed Are Electronic	479
iv.	Where the Environments in Which Special Categories of Personal Data Are Processed, Stored and/or Accessed Are Physical	481
v.	Transfer of Special Categories of Personal Data	482
vi.	The Need to Take into Account, in Addition to the Measures Mentioned, the Technical and Administrative Measures for Ensuring an Appropriate Level of Security Set Out in the Personal Data Security Guide Published on the Website of the Personal Data Protection Board	483
vii.	Other Measures, beyond the Minimum Level, to Be Taken by the Controller in View of the Purpose of Processing	483
b.	Data Breach Notification	486
i.	The Statutory Provisions and the Importance of the Subject	486
ii.	Who Is to Make the Data Breach Notification?	488
iii.	Time Limit for the Data Breach Notification	488
iv.	Points to Be Noted in the Data Breach Notification	490
v.	Failure to Make the Breach Notification at All or in the Proper Manner	492
c.	Failure to Take the Necessary Administrative and Technical Measures for Ensuring an Appropriate Level of Security in Order to Safeguard Personal Data Security	494
D.	Obligation to Register with the Data Controllers' Registry	500
1.	In General	500
2.	Exceptions to the Registration Obligation	501
a.	Exceptions Determined by Regulation	501
b.	Exceptions Determined by Decisions of the Board	502
E.	Erasure, Destruction or Anonymisation of Personal Data	504
1.	In General	504
2.	Methods and Measures Relating to Data Disposal	505
a.	Personal Data Retention and Disposal Policy	505
b.	Recording of Erasure, Destruction and Anonymisation and Retention of Those Records	506
c.	Method of Erasure, Destruction and Anonymisation	507
d.	Operations in Erasure, Destruction and Anonymisation	508
e.	Taking out of Use Data That Cannot Be Disposed of for Technical Reasons	513
f.	Time Limits for Ex Officio Erasure, Destruction and Anonymisation	515
g.	Time Limits for Erasure and Destruction upon Request	515
3.	Disposal of Personal Data in Outline	516
II.	OBLIGATIONS OF THE PROCESSOR	519
A.	Nature of the Processor	520
B.	Obligations of the Processor	522

C.	Principles to Be Observed by Virtue of the Relationship between the Controller and the Processor	524
1.	As Regards the Selection of the Processor	524
2.	As Regards the Continuation of the Guarantees Provided by the Selected Processor	524
3.	The Principle of a Written Contract	525

CHAPTER FOUR

CERTAIN SPECIAL ISSUES IN THE PROCESSING OF PERSONAL DATA

§ 12.	PROCESSING OF PERSONAL DATA IN THE EMPLOYEE–EMPLOYER RELATIONSHIP	527
I.	PROCESSING OF PERSONAL DATA IN RECRUITMENT PROCESSES	527
A.	Information and Documents That May Be Requested in the Recruitment Process	528
B.	Sharing of Personal Data Obtained in Recruitment Processes	529
C.	Continued Processing of Data after an Unsuccessful Job Application	530
II.	PROCESSING OF PERSONAL DATA BY MEANS OF ELECTRONIC MONITORING AFTER THE ESTABLISHMENT OF THE EMPLOYMENT RELATIONSHIP	532
A.	The Concept of Electronic Surveillance and Electronic Monitoring Practices Applied in the Workplace	532
1.	In General	532
2.	Reasons for Employers' Recourse to Electronic Monitoring Practices	534
B.	Processing of Personal Data by Means of Electronic Monitoring	537
1.	The Employer's Power to Monitor the Employee	537
a.	The Power to Monitor in General and Its Limits	537
b.	Monitoring of Employees' Work Computers, E-mails and WhatsApp Correspondence	543
i.	Whether the Employee May Use Means of Communication for Private Purposes	543
i.	Monitoring of Work Computers	547
ii.	Monitoring of Employees' Use of E-mail	548
iii.	Monitoring of Employees' WhatsApp Correspondence	552
c.	Monitoring of Employees' Entry to and Exit from the Workplace	554
d.	Monitoring of Employees by Security Camera	555
2.	Whether Data Obtained by the Employer through Electronic Monitoring May Constitute a Valid Ground for Termination	558
C.	Summary of the Subject in Outline and Our Assessments	561
III.	PROTECTION OF PERSONAL DATA AFTER THE TERMINATION OF THE EMPLOYMENT RELATIONSHIP	565
A.	Documents Submitted in an Action for Reinstatement	565
B.	Continued Processing of a Former Employee's Data	568
§ 13.	PROCESSING OF PERSONAL DATA IN MARKETING PROCESSES	570
I.	PROCESSING OF PERSONAL DATA IN MARKETING PROCESSES IN THE LIGHT OF THE DECISIONS OF THE BOARD	570
II.	SUMMARY OF THE SUBJECT IN OUTLINE	577
§ 14.	ARTIFICIAL INTELLIGENCE TECHNOLOGIES AND DATA PROTECTION LAW	579
I.	CONCEPTS RELATING TO THE SUBJECT	579
II.	ARTIFICIAL INTELLIGENCE AND THE PROCESSING OF PERSONAL DATA	582
III.	DATA PROCESSING BY ARTIFICIAL INTELLIGENCE UNDER PERSONAL DATA PROTECTION LAW	583
IV.	AUDIO, VISUAL OR WRITTEN MESSAGES GENERATED BY ARTIFICIAL INTELLIGENCE	588
§ 15.	PROCESSING OF PERSONAL DATA IN THE LEGAL PROFESSION: CONTROVERSIAL POINTS IN THE LIGHT OF THE DECISIONS OF THE BOARD	591
I.	IN GENERAL	591

II.	PROCESSING OF PERSONAL DATA IN THE COURSE OF PRACTISING THE LEGAL PROFESSION	591
A.	The Debate on Whether Lawyers Are Controllers or Processors	591
B.	Can Lawyers' Professional Activities Be Regarded as Falling within the Exception Laid Down in Art. 28(1)(d) of the Law on the Protection of Personal Data (KVKK)?	594
C.	The Obligation to Inform and the Obligation of Secrecy	596
D.	Inclusion of Personal Data in Pleadings Submitted to the Case File by Lawyers	597
E.	Sending of Garnishee Notices to Relatives of the Debtor	598

CHAPTER FIVE

PROTECTION OF PERSONAL DATA IN TURKISH CRIMINAL LAW AND THE LAW OF MISDEMEANOURS

§ 16.	PROTECTION OF PERSONAL DATA THROUGH CRIMINAL AND MISDEMEANOUR NORMS	601
I.	IN GENERAL	601
II.	THE NEED TO PROTECT PERSONAL DATA THROUGH CRIMINAL AND MISDEMEANOUR NORMS	601
III.	PROTECTION OF PERSONAL DATA IN THE TURKISH CRIMINAL CODE (TCK) AND THE KVKK	603
§ 17.	OFFENCES AIMED AT PROTECTING PERSONAL DATA IN THE TURKISH CRIMINAL CODE	604
I.	THE OFFENCE OF RECORDING PERSONAL DATA (ART. 135)	604
A.	In General	604
B.	Legal Interest Protected by the Offence	605
C.	Conformity with the Statutory Definition of the Offence (Tatbestandsmäßigkeit)	609
1.	Material (Objective) Elements of the Statutory Definition	609
a.	Perpetrator	609
b.	Victim	610
c.	Subject Matter of the Offence	611
d.	Conduct (Act)	614
e.	Result	615
f.	Aggravated (Qualified) Forms of the Offence	616
i.	Where Special Categories of Personal Data Constitute the Subject Matter of the Offence (TCK Art. 135(2))	616
ii.	Aggravated Forms Arising from the Status of the Perpetrator (TCK Art. 137(1))	617
2.	Mental (Subjective) Element of the Statutory Definition	618
D.	The Element of Unlawfulness	619
1.	Meaning of the Expression "Unlawfully" in the Definition of the Offence	619
a.	Our View on Expressions of This Kind from the Standpoint of the Theory of the Offence	619
b.	Our View on These Expressions in Arts 135 and 136 of the TCK	621
2.	Consent of the Victim	624
a.	The Time at Which and the Form in Which Consent Must Be Present	626
b.	Where the Personal Data Have Been Made Public by the Data Subject	627
c.	Cases in Which Explicit Consent Is Not Required for the Processing of Personal Data under Law No. 6698 (KVKK)	634
d.	Cases in Which Explicit Consent Is Not Required for the Processing of Special Categories of Personal Data under Law No. 6698 (KVKK)	635
3.	Reliance on Authority Conferred by Law	636
a.	Application of the Measure of Search and Seizure in Information Systems under the Code of Criminal Procedure (CMK)	636
b.	Processing of Personal Data within the Scope of the State's Intelligence Activities	637
c.	Evaluation of Signal Information under Article 135 of the CMK	639
d.	Processing of Health Data as a Special Category of Personal Data	644

4.	The Problem of Recording Information on Persons' Political, Philosophical or Religious Views and Racial Origins	645
5.	The Problem of the Fate of Personal Data in Information Systems Provided to Employees in the Public and Private Sectors	646
6.	Breach of the Obligations under the KVKK Does Not in Itself Constitute an Offence	646
E.	Special Forms of Appearance of the Offence	647
1.	Attempt	647
2.	Participation	648
3.	Concurrence	648
F.	Sanction, Investigation and Prosecution	652
II.	THE OFFENCE OF GIVING OR OBTAINING PERSONAL DATA (ART. 136)	652
A.	In General	652
B.	Legal Interest Protected by the Offence	652
C.	Conformity with the Statutory Definition of the Offence (Tatbestandsmäßigkeit)	653
1.	Material (Objective) Elements of the Statutory Definition	653
a.	Perpetrator	653
b.	Victim	653
c.	Subject Matter of the Offence	654
d.	Conduct (Act)	655
i.	Giving Personal Data to Another Person	661
ii.	Dissemination of Personal Data	663
iii.	Obtaining Personal Data	664
e.	Result	665
2.	Mental (Subjective) Element of the Statutory Definition	666
3.	Aggravated (Qualified) Forms of the Offence	671
D.	The Element of Unlawfulness	673
E.	Special Forms of Appearance of the Offence	675
1.	Attempt	675
2.	Participation	676
3.	Concurrence	676
F.	Sanction, Investigation and Prosecution	681
III.	THE OFFENCE OF FAILURE TO DESTROY PERSONAL DATA (ART. 138)	681
A.	In General	681
B.	Legal Interest Protected by the Offence	681
C.	Conformity with the Statutory Definition of the Offence (Tatbestandsmäßigkeit)	682
1.	Material (Objective) Elements of the Offence	682
a.	Perpetrator	682
b.	Victim	684
c.	Subject Matter of the Offence	685
d.	Conduct (Act)	685
i.	The Perpetrator Being Charged with the Duty and Allowing the Time Limit to Expire	685
ii.	Failure to Destroy the Data	686
e.	Aggravated (Qualified) Form of the Offence	687
2.	Mental (Subjective) Element of the Offence	689
D.	The Element of Unlawfulness	689
E.	Special Forms of Appearance of the Offence	690
1.	Attempt	690

2. Participation	690
3. Concurrence	690
F. Sanction, Investigation and Prosecution	691
IV. THE OFFENCE OF FAILURE TO ERASE OR ANONYMISE PERSONAL DATA PROVIDED FOR IN ART. 17(2) OF LAW NO. 6698 (KVKK)	692
§ 18. ADMINISTRATIVE SANCTIONS AIMED AT PROTECTING PERSONAL DATA PROVIDED FOR IN THE KVKK	693
I. IN GENERAL	693
II. ADMINISTRATIVE SANCTIONS PROVIDED FOR IN THE KVKK	694
§ 19. OUR ASSESSMENTS AND VIEWS ON THE PROTECTION OF PERSONAL DATA THROUGH CRIMINAL AND MISDEMEANOUR NORMS	696

CHAPTER SIX

THE PROCESS OF COMPLIANCE WITH PERSONAL DATA PROTECTION LEGISLATION

§ 20. THE PROCESS OF COMPLIANCE WITH PERSONAL DATA PROTECTION LEGISLATION	701
I. IN GENERAL	701
II. THE NEED FOR COMPLIANCE PROCESSES AND THE STATUTORY BASIS	702
III. THE COMPLIANCE PROCESS	707
A. Establishment and Implementation of the Compliance Strategy	707
B. Kick-off Meeting	707
C. Drawing up the Personal Data Inventory	707
D. Gap Analysis	710
E. Compliance Consultancy	711
1. Preparation of the KVKK Policy	711
2. Data Protection Officer/Committee	711
3. Finalisation of the Inventory and Registration with VERBİS	715
4. Explicit Consent Arrangements	716
5. Matters Relating to the Obligation to Inform	716
6. Data Protection Undertakings and Updating of Contracts	717
7. Transfer Abroad	718
8. Carrying out Data Minimisation and Disposal Operations	719
9. Determination of the Security Measures to Be Taken	720
10. Preparation and Updating of KVKK Policies and Procedures	720
F. Data Protection Consultancy after the Completion of the Compliance Process	727
IV. DATA PROTECTION TRAINING AND AWARENESS-RAISING	728
V. REVIEW	731
VI. ASSESSMENT AND OUR VIEW	732
Bibliography	735
Index	749

This document is the table of contents of the book, translated from Turkish; page numbers refer to the printed book. Page of the book: www.dulger.av.tr/en/publications/kisisel-verilerin-korunmasi-hukuku/