First Aid: General
Data Protection Regulation

Issued by the Data Protection Authority
of Bavaria for the Private Sector

C.H.BECK

General Data Protection Regulation:

First Aid for Companies and Associations

The Immediate Action Package for Germany

General Data Protection Regulation:
First Aid

What do organisations that hold or process personal data need to know?
From 25th May, 2018, the European Union's General Data Protection Regulation, GDPR for short, applies. It creates a completely new basis for all data protection in the European Union. The fines for breaches have been drastically increased.

In addition to large enterprises and other types of large scale organisation, small companies or free-lancers, small associations, clubs, societies and non-profit making organisations in many shapes and forms are entrusted with a lot of personal data - be it customer or client data, member data, employee data, or supplier data. Clubs and associations often have documentation that allows deep insights into the personal situation of their members. All organisations which hold or process this type of data are defined as "controllers" under the GDPR. It is therefore essential for the respective "controllers" to know the requirements of the GDPR.

This publication informs you concisely and clearly regarding the content and the mandatory requirements relating to data processing in the GDPR. In particular it answers the following questions:

- Which **data** is covered by data protection?
- Is it necessary to nominate a **Data Protection Officer**?
- Which **obligations to provide information** must be fulfilled pro-actively?
- What information needs to be included in the **records of data processing activities**?
- When is it permissible to **forward data** to other persons or organisations?
- Which special requirements are there for **photographs on your own website?**

Templates and check lists help you prepare and implement the legal requirements of the General Data Protection Regulation. Numerous examples demonstrate legal pitfalls and how to avoid them.

This publication is aimed at owners of small companies, those responsible for data protection within small companies, chairpersons and members of clubs or associations and many other types of non-profit making organisation, as well as anyone else who wishes to gain a quick overview of the requirements of the data protection legislation.

About the authors
This publication was created by data protection experts. **Dr. Eugen Ehmann** is Vice-President of Central Franconia (Bavaria) and co-author of Ehmann/Selmayr, Kommentar zur DS-GVO (Commentary on the GDPR). Thomas Kranig is President of the Data Protection Authority of Bavaria for the Private Sector.

General Data Protection Regulation: First Aid for Companies and Associations

The Immediate Action Package for Germany

Issued by the Data Protection Authority of Bavaria for the Private Sector

Authors:

Thomas Kranig, President of the Data Protection Authority of Bavaria for the Private Sector

and

Dr. Eugen Ehmann, Vice-President of Central Franconia (Bavaria)

Translated by Julia and Brent Ellis-Simpson

Foreword

On 25th May, 2018, uniform data protection legislation takes effect in the European Union. It is set out in the General Data Protection Regulation (GDPR). The specific requirements are very similar to previous legal requirements in Germany. Nevertheless, there is a series of new requirements which it is important to implement. They are to be implemented literally “overnight” on 25 May 2018. The legal form of the new data protection legislation is unusual in that the new Data Protection Act has been enacted in the form of an EU Regulation. Such EU Regulations are valid and have immediate effect in and on all member states of the EU. Transposition of regulations of this nature by the legislative bodies of the EU member states is not necessary anymore. However, where permitted by the Regulation, national legislative bodies may stipulate additional supplementary requirements.

Also new is that this EU law has empowered the Data Protection Supervisory Authorities to impose fines for breaches of this Regulation of up to EUR 20 million, or alternatively fines of up to 4 % of annual global turnover for enterprises. For this reason alone, it is well worthwhile immediately familiarising yourself with the requirements of the new data protection legislation.

This publication is aimed mainly at small companies, free-lancers and associations. These organisations or people are definitely not “data protection specialists”, but are constantly dealing with employee, customer/client, patient or member data. They do not usually have a legal department to support themselves or their management. However, they need to ensure that all personal data is dealt with in accordance with the GDPR. This publication aims to help you to do that. It cannot and does not aim to do more than give an overview of what the legal requirements which apply from 25th May, 2018 will actually be. It also aims to make clear what small companies, free-lancers, associations and similar organisations need to arrange, in order not to get into trouble.

To make it easier, we have sometimes added check lists or templates. These should give you an idea of the things you need to think about in each case. It should be noted, however, that they are only templates, and cannot cover all cases.

If you, the reader, should notice that in your case the requirements of the GDPR are more complex than we can demonstrate in this publication, then please refer to the information sources listed at the end of this publication. If that is still not sufficient, you can seek professional advice from a data protection expert. That will cost you money, but it may also save you a lot of trouble. For specific individual issues, you may also consult your local supervisory authority.

The aim of this publication is to raise awareness, in you the reader, of what you need to do. At the same time, it should act as an initial source of advice. In order to achieve these aims, we sometimes address you personally. We hope that this will make you particularly aware that you are personally responsible for deciding which topics are relevant for you, and what you are required to do in these cases.

We would like to express our heartfelt thanks to Daniela Duda, whose constructive criticism was of invaluable help in creating both text and tables.

Eugen Ehmann and Thomas Kranig

Table of Contents

Chapter 1: Scope of the General Data Protection Regulation (GDPR) 9

Chapter 2: First Steps 10

Chapter 3: Records of Processing Activities 12

1. Duty to establish documentation 12
2. Exemption from the duty to establish documentation 12
3. Submission of records 12
4. Form of records 12
5. Updating the records 12
6. Content of records 12
7. Extended records 13
8. Template for records of processing activities 13

Chapter 4: Principles of Processing Personal Data 21

1. Prohibited unless authorised 21
2. Lawfulness 21
3. Purpose limitation 22
4. Accuracy of the data 22
5. Necessity of storage 22
6. Principle of accountability 23

Chapter 5: Processing on Behalf of a Controller 24

1. The limits of “processing on behalf of a controller” 24
2. Selection of processor 24
3. Contractual provisions 24
4. Supervisory rights 24
5. Ending the processing on behalf of a controller 24

Chapter 6: Security of the Processing . . . 25

1. IT security . . . 25
2. Protection aims of IT security . . . 25
3. IT security as a top level management issue . . . 26
4. Management of rights and permissions . . . 27
5. Identifying and addressing risks . . . 27
6. Everyday encryption . . . 28
7. Patch management . . . 29
8. Using email communication correctly . . . 29
9. Blocking malware: backups . . . 29
10. Impeding and barring access . . . 30
11. Typical misconceptions about IT security . . . 30

Chapter 7: Data Protection Officer . . . 32

1. Purpose of nomination of a Data Protection Officer . . . 32
2. Duty of nomination . . . 32
3. Voluntary nomination of a Data Protection Officer . . . 35
4. Nomination of an internal or external Data Protection Officer . . . 35
5. Formal requirements for nomination . . . 35
6. Duties of the Data Protection Officer . . . 37
7. Informing the supervisory authority . . . 37
8. Publication of contact details of the Data Protection Officer . . . 39

Chapter 8: Rights of Data Subjects (Data Subject Rights) . . . 40

1. Transparent information . . . 40
2. The right to access . . . 40
3. Rectification, erasure and limitation of processing . . . 41
4. Data portability . . . 41
5. Right to object to the processing . . . 41

6. The right not to be subject to decisions based on automated processing 42

7. In summary 42

Chapter 9: Personal Data Breach 43

1. Overview of the regulations 43

2. Clarification of the term “personal data breach” 43

3. Obligation to notify the supervisory authority 44

4. Duty of communication of a personal data breach to the data subject 45

5. Details on communication to the data subject 46

Chapter 10: Sanctions and Liability 47

1. Overview 47

2. Fines stipulated in the Regulation 47

3. Compensation and liability 47

Chapter 11: Requirements Concerning your own Enterprise Structure 48

1. Implementation of accountability 48

2. Requirements 48

3. Responsibility for data protection issues 48

4. Defining a cycle for checking data protection issues 48

Chapter 12: Co-operation with the Supervisory Authority 49

1. Entitlements vis-à-vis the supervisory authority 49

2. Responsibilities and powers of the supervisory authorities 49

Chapter 13: Dealing with Photographs in the Internet 50

1. Technical background 50

2. Legal background 50

3. Images on websites of enterprises 52

4. Images on websites of associations 55