dormakaba

EU General Data Protection Regulation

Guidelines for products, services and applications with personal data.

Version:	1.1
Status:	Released
Release Date:	09.05.2018
Classification:	Public

Contents

1 About this document

1.1 Objectives

This document describes requirements and measures as a recommendation for the implementation of the European General Data Protection Regulation [1] in the context of products, services or applications that process personal data, such as systems for access control and T&A.

The dormakaba EAD EMEA access control systems (see 3.2 Current dormakaba EAD systems) are configurable. Steps for the configuration of the system in accordance with the GDPR are listed under ‘technical measures’.

In the context of dormakaba system solutions, the objective is to support our customers with regard to the implementation of the General Data Protection Regulation and to propose technical and organisational measures [7] for compliance with the regulation.

In the case of all on-premise solutions [5] (for a list, see section 3.2), the customer’s data controller [8] is responsible for compliance with legal requirements and for the correct implementation of the GDPR. In the case of dormakaba’s software as a service (SaaS) solutions, dormakaba, as the processor [9], shares this responsibility. The requirements for the SaaS solutions with regard to the GDPR and the formulation of the contractual terms with SaaS customers will be considered separately.

Please note the disclaimer below for all system solutions. (1.4)

1.2 Scope of the GDPR

The content of this document concerns the European General Data Protection Regulation [1] and applies, in accordance with Article 2 of the GDPR 'Material scope', to the processing of personal data stored in a filing system. In accordance with Article 4 of the GDPR, "any information relating to an identified or identifiable natural person" is covered by the regulation.

In accordance with Article 3 of the GDPR 'Territorial scope', the regulation applies to EU enterprises: "The GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller [8] (an enterprise) or a processor [9] in the Union, regardless of whether the processing takes place in the Union or not". The GDPR applies to all enterprises and organisations in the EU, but not to private persons.

Enterprises outside the EU (CH): In accordance with the principle of the place of performance (Article 3(2) of the GDPR), the regulation is also applicable to enterprises or processors based outside the EU, e.g. to enterprises in Switzerland. If, for example, a company processes customer data and exchanges it with the IT data centre in Switzerland, the EU GDPR will also apply there.

1.3 Scope of this document and disclaimer

This document concerns the handling of "personal data" [3] in the context of products, services or applications that process personal data

in accordance with the General Data Protection Regulation [1].

Disclaimer: Please note that this document only summarises the most important contents of the GDPR in the context of the dormakaba system solutions mentioned above. This document does not constitute legal advice and is not intended to replace an appropriate consultation with regard to compliance with the statutory data protection regulations in a company. No liability is assumed for the accuracy, completeness or topicality of the information (including references to other sources).

Many aspects of the GDPR refer to processes, training, contractual arrangements and roles of employees, which must be defined and monitored by the operator's data controller [8]. Likewise, conformity assessment procedures are the responsibility of the operators or their data controllers.

2 Measures

2.1 Identify and document processing activities

DESCRIPTION	**Identify processing activities concerning personal data** [3] in the enterprise and **answer key questions** (data controller, types of data, source of data, data transfer etc.). Mandatory for enterprises with more than 250 employees.
OBJECTIVE	• Identify processing activities • Ensure evidence of processing activities
ORGANISATIONAL MEASURES BY CUSTOMER	**Identify processing activities** • Applications • Systems • Document repositories (e.g. Excel files), records **Key questions per processing activity:** • In which legal entities/locations/departments is the processing activity carried out? • Who is responsible for the processing activity in question? • Which personal data of which persons is processed? • For what purpose is the data processed? • Legal basis for the collection of personal data (e.g. addition to employment contract, declaration of consent)? • Where does the data come from (origin)? • Where does the data go/to whom is the data sent? • Time limits for erasure: For how long is the data required/stored? **Document processing activities as evidence.**
CONFIGURATION OF DORMAKABA SYSTEMS (TECHNICAL MEASURES)	Identifying and documenting processing activities is a fundamental organisational measure on the part of the customer. With the processing activities, the customer must also consider and document the dormakaba systems, services or products with personal data, including data flows (interfaces) to other systems.
REFERENCE	Article 30 GDPR

2.2 Ensure compliance with data protection principles

DESCRIPTION	**Data protection (privacy) by design and by default:** Implement data protection principles (e.g. data minimisation) through both technical measures (e.g. software) and organisational measures (e.g. organisational processes). **'Privacy by design':** Data protection problems are already identified and checked during the development of new technologies. Data protection is included from the outset in the overall design.

	'Privacy by default': Products or services are, by default, delivered or configured in a privacy-friendly manner.
OBJECTIVE	• Processing of personal data with the least risk for the data subjects. Data minimisation and purpose limitation – the data collected must be appropriate for the purpose and limited to what is necessary for the purposes of processing.
ORGANISATIONAL MEASURES BY CUSTOMER	• **Review of existing statutory or contractual storage obligations**. Personal data is stored only for the duration of the actual purpose (e.g. access for the duration of the employment relationship) – beyond that only if there are corresponding statutory or legally binding storage obligations. **Implementation:** Configure systems in such a way that data that is no longer required will be deleted automatically. • **Create transparency with regard to the functions and processing of personal data.** **Implementation:** Provide information that makes the purpose and the data collected transparent to users (employees, visitors, contractor employees). • **Minimise access to personal data Implementation:** Restrict access rights. Assign access rights to personal data only to required persons (roles). • Check that only personal data that is actually required is being processed for a specific purpose. • **Anonymise data if it is to be used for testing, analysis or documentation purposes etc.** • **Implementation:** Anonymise personal data on its removal from production systems. Separation of test and production systems.
CONFIGURATION OF DORMAKABA SYSTEMS (TECHNICAL MEASURES)	• **Minimise the quantity of personal data.** **Implementation:** Existing configuration options are factory-set to privacy-friendly values. By default, minimal personal data is displayed: e.g. last name, first name, image of the person, staff number, department, entry date, media, authorisations (system-dependent). • Configure other fields (e.g. date of birth) according to customer requirements and only display if required. • **Delete personal data as early as possible.** **Implementation:** Automatic deletion when the personal data is no longer required for the purpose for which it was collected, e.g. employee, visitor or contractor employee data after their exit and a specified time period. This includes personal log or T&A data. The retention limit should be configured to an **appropriate value**, e.g. 90 days for access data or 1 year for T&A data; see also organisational measures by the customer. • **Anonymise personal data.** **Implementation:** Anonymise personal data when it is removed from production systems, e.g. by means of database scripts. Fully anonymised

	data is no longer subject to the GDPR and can thus be exchanged with third parties. • **Minimisation of access to personal data. Implementation:** Restrict visibility of personal data (e.g. extended personal data with image of the person, date of birth, entry date, media, authorisations, mobile phone, vehicle licence plate); link access to dedicated user rights (roles). This applies in particular to the evaluation and exporting of personal data.
REFERENCE	Article 5 GDPR Principles relating to processing of personal data Article 25 GDPR Data protection by design and by default

2.3 Protect the rights of the data subject

DESCRIPTION	In addition to the data controller's [8] expanded duties in accordance with Articles 12, 13 and 14 of the GDPR (transparency and information), the data controller must also observe the data subjects' comprehensive rights and ensure that these are implemented in good time when they are asserted.
OBJECTIVE	• Right of access (Article 15 GDPR) • Right to rectification (Article 16 GDPR) – correction of inaccurate data • Right to erasure or "right to be forgotten" (deletion without trace, Article 17 GDPR) • Right to restriction of processing (Article 18 GDPR) For the period necessary to verify data or protect against legal claims. • Notification obligation regarding rectification or erasure of personal data or restriction of processing (Article 19 GDPR) • Right to object (Article 21 GDPR)
ORGANISATIONAL MEASURES BY CUSTOMER	• Inform employees (e.g. Human Resources department, reception staff) about the rights of data subjects in accordance with the GDPR and ensure implementation. • The data controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data has been disclosed.
CONFIGURATION OF DORMAKABA SYSTEMS (TECHNICAL MEASURES)	• **Provision of a copy of the relevant personal data. Implementation:** Provide a screenshot, evaluation or export of the data stored for a person. Additional information: purpose, recipient, duration of storage, data subject's rights[1], source of the data, tracking of movements (access logs), any transfer to third countries.

[1] Example of data subject's rights: "In accordance with the European General Data Protection Regulation (GDPR), you have the right to a copy of your stored personal data. Furthermore, in accordance with the GDPR, you may at any time request the rectification, erasure or

	• **Right to erasure and right to object** **Implementation:** Manual deletion of employee, contractor or visitor data (if no longer required), including associated log data. • **Right to restriction of processing** **Implementation:** It must be possible to exclude data from processing without deleting it. Locking records, manual blocking of the person (access rights). • **Right to "be forgotten"** **Implementation:** Automatically delete data if the personal data is no longer required for the purpose for which it was collected. (E.g. employee, visitor or contractor employee data after their exit and a specified time period; see also compliance with data protection principles)
REFERENCE	Articles 12–23 GDPR on rights of the data subject

2.4 Introduce a consent process

DESCRIPTION	The lawfulness of the processing of personal data, insofar as it is not for the purpose of fulfilling a contract or a legal obligation, may be ensured in particular by the consent of a natural person.
OBJECTIVE	• Consent should be given by a voluntary, clear action which signifies that the data subject agrees to the processing of their personal data
ORGANISATIONAL MEASURES BY CUSTOMER	• Obtain agreement with the storage of personal data where no contract is in place, e.g. through the signing of a form in the case of visitors or contractor employees. The data controller [8] must be able to prove that the data subject has consented to the processing of their personal data. • This consent can be withdrawn at any time. In that case, the personal data must be deleted (see also 2.3 Protect the rights of the data subject). • Arrange contractual employment provisions with employees, with corresponding information on rights and obligations. **Note on data minimisation/purpose limitation:** Even if consent has been provided for the storage of personal data, the principles regarding data minimisation and purpose limitation in accordance with Article 5 of the GDPR must be observed.

restriction of the processing of your data. If your data is erased, all access rights will expire and any user media or keys must be returned. The data is collected only for the purpose of access control and security and is automatically deleted after nn days."

	Note on existing data: Please be aware that consent must be obtained for future personal data as well as for personal data that has already been collected.
CONFIGURATION OF DORMAKABA SYSTEMS (TECHNICAL MEASURES)	• For example, store a signed visitor pass with consent; in the case of self-registration (e.g. contractors or visitors) via the web portal, store the (active) declaration of consent**.**
REFERENCE	Article 6 GDPR Lawfulness of processing Article 7 GDPR Conditions for consent

2.5 Introduce a duty to provide information

DESCRIPTION	In order to ensure the fair and transparent processing of personal data, the data controller must provide data subjects with all information that describes the nature, purpose and extent of the processing activity. In this respect, a distinction is made between data that is collected directly from the data subject and data that becomes available to the data controller by other means.
OBJECTIVE	• Creation of accurate, easily accessible information on the personal data processing activity carried out, that can be easily understood by the data subject
ORGANISATIONAL MEASURES BY CUSTOMER	If the data is collected directly from the data subject, the following information should be provided at the time of collection: • Name and contact details of the data controller [8] and, if applicable, of their representative and, if applicable, of the data protection officer [2]. • The purposes for which the personal data will be processed (access control, security) • The storage duration of the data or the criteria for determining this duration • A reference to the data subject's rights to access, rectification, erasure, objection and data transfer (see also • Protect the rights of the data subject).
CONFIGURATION OF DORMAKABA SYSTEMS (TECHNICAL MEASURES)	Can be covered by organisational measures on the customer's side.
REFERENCE	Article 12 Transparent information, communication and modalities for the exercise of the rights of the data subject Article 13 GDPR Information to be provided where personal data are collected from the data subject

2.6 Implement data security measures (TOMs)

DESCRIPTION	The data controller [8] must take appropriate technical and organisational measures [7], depending on • **the state of the art** • **the costs of implementation** • **the scope, context and purposes of processing** as well as • the **risks of varying likelihood and severity** for the rights and freedoms of natural persons. The state of the art is generally represented by internationally recognised standards (e.g. ISO/IEC 27001:2013, BSI IT Baseline Protection). These specifications must be adapted to the circumstances of the individual organisation.
OBJECTIVE	• Ensure suitable TOMs • Compliance with the state of the art
ORGANISATIONAL (TECHNICAL) MEASURES BY CUSTOMER	Which TOMs are to be implemented? (in accordance with the controls of ISO/IEC 27002) • Central information security requirements • Draw up IT security or user policy (e.g. security policy, data protection policy) • Draw up password requirements • Define roles and responsibilities • Draw up processes for entry, team change and exit • **Management of values (e.g. devices, software, authorisations, keys),** responsibilities and rules for return • **Physical access arrangements (e.g. keys, access control)** • **Define rules for access (e.g. user management, access to systems)** • Define measures for installing software (e.g. regulation of administrator rights) • Ensure data security and recovery (database systems) • Logging and monitoring mechanisms • **Physical and environment-related security** • **Define security zones (e.g. fence or access control for data centre)** • Network security measures (e.g. firewall, network segmentation, 802.1X) • Communication security • Separation of development, test and production systems • **Process for handling security incidents** (attack, data loss or disclosure, Article 33 GDPR)
CONFIGURATION OF DORMAKABA SYSTEMS (TECHNICAL MEASURES)	Set up in accordance with customer's specifications: • Access protection (user roles and authorisations) • Password policy, if configurable, or use SSO (one- or two-factor authentication) • Logging mechanisms (access, media, audit, system logging): data capture, change, query, disclosure /export/transfer, with user, date/time and reason, if applicable. • Confidentiality and data integrity via database encryption (e.g. transparent data encryption or column-level encryption). • Secure storage of passwords or keys.

	• Secure data transmission (confidentiality, integrity and authenticity) according to customer's requirements. This applies in particular to transmission via unsecured networks or over the internet.
REFERENCE	• Article 32 GDPR Security of processing • ISO/IEC 27001:2013 and the controls of ISO/IEC 27002:2013 • BSI IT Baseline Protection

2.7 Perform a risk analysis

DESCRIPTION	The data controller [8] should carry out a **risk assessment for the identified risks of the processing activities** (estimation of likelihood and effects). If **there is likely to be a high risk to the data subjects**, a data protection impact assessment should be carried out.
OBJECTIVE	• Analyse the effects and risks of processing activities for the rights of data subjects • Risk assessment per processing activity ▪ Likelihood ▪ Effect/damage
ORGANISATIONAL MEASURES BY CUSTOMER	Guidelines for risk assessment (customer's data controller) in accordance with the specifications of the Article 29 Data Protection Working Party: 1. Evaluation or scoring, including profiling and making predictions 2. Automated decision-making with legal or similarly significant effects for data subjects 3. Systematic monitoring 4. Sensitive personal data 5. Data processed on a large scale 6. Datasets that have been matched or combined 7. Data concerning vulnerable data subjects 8. **Use of innovative technologies (which includes biometrics, according to the GDPR**) or novel organisational solutions **9. Data transfers to countries outside the EU** 10. Preventing data subjects from exercising a right or using a service or a contract **Based on the recommendations of the above group, a risk assessment should be carried out as soon as a processing activity meets two or more criteria.**

	Biometrics: In accordance with Article 9 of the GDPR, biometric data for the purpose of uniquely identifying a natural person falls under special categories of personal data [4 Special categories of personal data]. The processing of this data is permitted only for the exceptions specified in Article 9(2). In accordance with Article 35(1) of the GDPR, a "data protection impact assessment" is required for the processing of special categories of personal data. **Exception:** The data subject has given explicit consent to the processing of the aforementioned personal data for one or more specified purposes. **Implementation:** The data controller must be able to prove that the data subject has consented to the processing of their data (for the purpose of access control or T&A). On collection (biometric enrolment), ask for the explicit consent of users and get them to sign a form, for example. (The customer may, if applicable, offer persons who refuse biometric enrolment a badge as an alternative or may deny them access.) For special categories of personal data, such as the (central) storage of biometric data, a risk assessment should be carried out and data security measures (e.g. encrypted storage; see section 2.6) should be implemented. **Data transfers to countries outside the EU:** The transfer of personal data to third countries is permitted only under defined conditions. Any transfer of personal data (which has already been processed or which is to be processed after its transfer to a third country or an international organisation) is permitted only if the data controller and the processor comply with the conditions laid down in this section and the other provisions of this regulation in accordance with Articles 44–50 of the GDPR. (It should be noted, however, that the movement of data within the EU must not be hindered.) **Implementation:** Check, and if necessary restrict, the transfer of personal data. Configure systems (access rights, tenants) in such a way that the personal data of EU citizens is not transferred to third countries.
CONFIGURATION OF DORMAKABA SYSTEMS (TECHNICAL MEASURES)	-
REFERENCE	• Article 35 GDPR Data protection impact assessment • Articles 44–50 GDPR Transfers of personal data to third countries or international organisations

2.8 Introduce a data breach process

DESCRIPTION	A process is to be introduced for the timely notification of data breaches and the timely taking of appropriate countermeasures.
OBJECTIVE	• Define correct behaviour in the event of a data breach • Correct and timely information to third parties
ORGANISATIONAL MEASURES BY CUSTOMER	Preparation for a data breach (the first step is to define all the activities, so that they can be implemented quickly in case of need): • Identify process dependencies and available resources • Define roles and responsibilities o What are the roles covered by the Computer Emergency Response Team (CERT)? • Detect and record incident • Perform initial assessment • Take emergency measures • Information to the data controller • Information to the data subjects: o Written in clear and plain language o Description of the nature of the personal data breach o Approximate number of personal data records concerned o Name and contact details of the DPO or other point of contact where more information can be obtained o Description of the consequences of the personal data breach o Description of the measures taken by the data controller • **Information to the supervisory authority within 72 hours** o Minimum information to the supervisory authority: Description of the nature of the personal data breach, including where possible: o The categories of data subjects concerned o The approximate number of data subjects concerned o The categories of personal data records concerned o The approximate number of personal data records concerned o Name and contact details of the DPO or other point of contact where more information can be obtained o Description of the consequences of the personal data breach o Description of the measures taken or proposed by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects o Documentation of all personal data breaches, including the facts relating to the breach • Taking of (follow-up) measures
CONFIGURATION OF DORMAKABA SYSTEMS (TECHNICAL MEASURES)	-
REFERENCE	• Articles 33 and 34 GDPR

3 Additional information

3.1 Definitions, acronyms and abbreviations

Term	Description
1 GDPR	https://dsgvo-gesetz.de/ https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
2 DPO	Data protection officer
3 Personal data	According to the EU General Data Protection Regulation (GDPR), personal data is all information that relates, or at least may be related, to a natural person and thus allows conclusions to be drawn about their personality. A natural person is considered to be identifiable if they can be identified directly or indirectly, in particular by association with an identifier such as a name, with an identification number, with location data, with an online identifier or with one or more special features. In the context of access control, personal data includes, for example, last name, first name, date of birth, gender, image of the person, mobile phone, e-mail, vehicle licence plate, but also log data (e.g. access logs) relating to the person.
4 Special categories of personal data	In accordance with Article 9 of the GDPR, *special categories of personal data* are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic **or biometric data** for the purpose of uniquely identifying a natural person**,** data concerning health or data concerning sexual orientation**.** The processing of this data is prohibited and permitted only for the exceptions specified in Article 9(2).
5 On-premise	With the commercial on-premise software model, customers purchase or rent software and operate it under their own responsibility on their own hardware, possibly in their own data centre or on rented servers in a third-party data centre, in any case therefore on hardware that is not provided by the software vendor.
6 SaaS	The SaaS model is based on the principle that the software and the IT infrastructure are operated by an external IT service provider and are used by the customer as a service. An internet connection to the external IT service provider is required for the use of online services.
7 TOMs	Technical and organisational measures required to meet the data security and protection requirements.
8 Data controller	A data controller is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
9 Processor	The processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

	Examples: A businessperson who collects customer data (from natural persons) in order to prepare an invoice to be sent to the customer is a 'data controller'. An external accountant who receives and processes the invoice data in order to prepare financial reports for this businessperson is a 'processor'. Other examples of a 'processor': data centre, payroll accountant, cloud provider etc.

3.2 Current dormakaba EAD systems

System	Description	Usage model
B-COMM®	B-COMM integration platform	On-premise
b-comm-ERP®	b-comm ERP integration platform	On-premise
b+	b+ integration platform	On-premise
EACM	Enterprise Access Control Management – access solution in SAP	On-premise
evolo smart	Kaba evolo smart – access solution for small businesses/residential	On-premise
exivo	Kaba exivo – cloud-based access solution	Software as a service (SaaS)
exos 9300	Kaba exos 9300 – access solution for medium-sized and large enterprises	On-premise
exos 9300 SBS	Kaba exos 9300 access solution – small business solution for medium-sized enterprises	On-premise
KEM	Kaba exolo Manager	On-premise
MATRIX ONE	MATRIX One – access solution for small and medium-sized enterprises	On-premise
MATRIX PRO	MATRIX Professional – system solution for access control, time registration and T&A	On-premise

3.3 Related documents

Ref.	Description

3.4 Versions

Ver.	Author	Modifications	Date
0.1	Markus Fischer	Draft created	16/02/2018
0.2	Markus Fischer	Additions, focus on target group: Sales, PMM	26/02/2018
0.3	Markus Fischer	Additions pursuant to review feedback	28/02/2018
0.9	Markus Fischer	Additions and information from Group Legal feedback and TÜV Rheinland	06/04/2018
1.0	Markus Fischer	Additions and information from project team review	09/04/2018

1.1	Markus Fischer	Public version created	09/05/2018

Ver.	Inspected by	Role/title	Signature	Date
02	Bastian Moeller	Group Legal		04/04/2018
02	Hans-Werner Geerts	TÜV Rheinland		04/04/2018