arvato
BERTELSMANN

# White Paper

# General Data Protection Regulation (EU- GDPR)

## Essential content and implementation in the Arvato Systems Group

## Legal notice



This document is of a purely informative character and in particular does not constitute legal advice or legal information and does not claim to be exhaustive with regard to all aspects necessary for the legally compliant implementation of the General Data Protection Regulation.

## Table of contents

# 1 EU General Data Protection Regulation

## 1.1 Introduction

The aim of this document is to clarify the significant innovations that will come into force with the EU General Data Protection Regulation (GDPR) and to illustrate the joint implementation of legal data protection requirements within the Arvato Systems Group.

For many years, Arvato Systems has acted on behalf of clients from sectors that place the highest requirements on the management and processing of their data. These include clients from the energy, banking, insurance or healthcare sectors as well as from the media, utilities and trading/e-commerce sectors who process types of personal data listed as special by the General Data Protection Regulation (GDPR) or who outsource high-security-level data processing to Arvato. Due to the resulting enormous demands regarding data protection, the Arvato Systems Group was well prepared for the regulation's entry into force on May 25, 2018. At the same time, we recognize the challenges posed by the innovations (partly still in uncertain legal situation) to all responsible agents in companies when it comes to use current technologies to protect the high value of personal data and the privacy in the best way on the behalf of our customers.

## 1.2 Basic principles of the GDPR (DSGVO in German)

With the GDPR, the European legislature is taking account of the need to create a uniform data protection basis within the European member states in a world that is undergoing globalization and digitization. Previously valid national laws on data protection - such as the German Federal Data Protection Act (BDSG) - were replaced in key areas by the new EU regulation. At the same time, the GDPR contains flexibility clauses; these allow member states to determine supplementary or deviating national regulations.

With the new Federal Data Protection Act (BDSG) and the Data Protection Adaptation and Implementation Act the German legislature was the first European Member State to make use of the GDPR's dissemination in April 2017. The amendments made to the previous German Federal Data Protection Act (BDSG) and to the GDPR are only partly of essential importance for non-public companies (e.g. data protection responsibilities, scoring and creditworthiness, § 31 (new) German Federal Data Protection Act (BDSG), video surveillance, § 4 para. 2 (new) German Federal Data Protection Act (BDSG): contact details are also to be made identifiable). Details will not be entered into here, especially since the interaction between the GDPR and the (new) German Federal Data Protection Act (BDSG) as well as other special laws are already controversial, and parts of the (new) BDSG have already been criticised as being contrary to European law. For now it remains uncertain and exciting which specific implementation requirements will arise from this debate.

In Germany and other European member states, further supplementary national regulations are still awaited. Special regulations, such as the German Social Security Code (SGB) and Telecommunications Act (TKG), will continue to apply. One consequence is that the GDPR always has to be considered in conjunction with various national legislations, in order to take account of legislative requirements. This means that internationally trading companies will continually have to reckon with the data protection regulations of the respective EU countries when offering their goods and services to and for these markets. It is expected that the e-privacy regulation, which is still at the design stage, will also have an impact on data processing.

With regard to the GPDR, which operates in many places with undefined legal rights, companies in Germany are hoping that the federal states' supervisory authorities will continue to offer guidance for its implementation in their organization.

These means of assistance are only a basic guide for the implementation of GDPR requirements into business practice. However, a well-founded legal debate on the interpretation has just begun. State commissioners are pointing out that the binding and uniform interpretation of the GDPR is made solely by the European Data Protection Board and the courts.

The practical interaction and substantiation of national supervisory authorities as well as national supplementary data protection laws are still missing; in many places, the implementation of the GDPR poses major questions to even experts, and there is great uncertainty amongst many companies regarding the specific measures to be taken. One thing is certain, however: the companies, i.e. *the responsible parties*, must deal with the new regulations and review existing data processing, processes, customer and supplier contracts and, if necessary, adapt them and make alterations. As an incentive, the provisions for fines in Articles 82-84 of the GDPR is certainly not insignificant.

## 1.3 Important contents/changes at a glance

In total, the GDPR has 99 articles. The following report provides an overview of the essential requirements contained therein, together with their recitals:[1]

### 1.3.1 Basic principles/prohibition with reservation of authorization

Basic principles of data protection, such as basic prohibition of processing personal data with reservation of authorization and the need for data minimization and data security, will remain in place. The documentation obligations imposed by the GDPR on responsible parties will be increased and data subjects' rights are also strengthened (e.g. right to be forgotten, rights to information, data protection-friendly default settings, data portability).

The essential guiding principle of data protection is that any processing of personal data requires authorization. There are many alternatives to consider when it comes to authorization. First of all, there is the data subject's authorization; their **consent**. However, statutory authorizations can be obtained from the **standards** of the GDPR as well as from national regulations. Special conditions for the consent of children are laid down in Article 8 of the GDPR. The obligation to prove the existence of consent lies with the responsible parties; they must hereby also observe the usual principles, such as the transparency requirement and information obligation. Therefore, the consent of a data subject, who has been sufficiently informed in advance, constitutes a voluntary and unequivocal declaration of will. This information must also specify that the data subject can revoke their consent at any time with future effect.

However, the legality of the processing may also be founded upon the necessity of **contractual performance** or **pre-contractual measures** - in such a case, no explicit consent is required from the data subject.

With its possibility to process data on the basis of a **weighing of interests**, **Article 6 para. 1 lit. f. GDPR** is a special authorization standard that is worthy of mention. It is clear from the recitals that, in principle, corporate group interests must also be included in the weighing of interests; this article should not be misunderstood as a general group privilege, however.

Special requirements must be set when processing specific categories of personal data (e.g. ethnic origin, religion, health, biometric identifiers) (Article 9 GDPR). Special restrictions also apply to data regarding criminal convictions or offences.

[1] Please note that the statements do not constitute legal advice or legal information and do not claim to be exhaustive.

If data processing is initially carried out in a lawful manner, a limited **processing permit** is then possible, as long as this intended for compatible purposes. The responsible party must therefore be able to prove that the later purpose is compatible with the original one.

### 1.3.2 Lex loci solutions

The GDPR's scope of application also extends to non-European companies, provided they offer their services in the EU. A responsible processor without a branch in the EU must appoint a representative in the EU as a point of contact for data subjects and supervisory authorities. This means that, for the first time, foreign companies and processors (for example, public cloud providers such as Amazon, Salesforce, Facebook or Microsoft) are covered by EU legislation and must also meet the requirements of the GDPR for their products and solutions.

### 1.3.3 "One-Stop-Shop mechanism"

From now on it is clear that, when it comes to a company's cross-border data processing in several EU countries, the sole responsible supervisory authority for this will the one based at EU headquarters.

### 1.3.4 Accountability

The responsible party – normally the company that collected the data and either processed it itself or had it processed on its behalf – is responsible for compliance with data protection principles or relevant laws and must be able to prove its compliance. Overall, the GDPR increases documentation requirements. Documentation and proof obligations are comprehensive and require a professional data protection management system.

### 1.3.5 Transparency requirements

Information and disclosures must be made available to the data subject in writing in easily understandable language and generally free of charge. The data subject must be able to know who is processing which data about him/her and for what purposes. The requirement for transparency is thus reflected in many requirements and covers the entire chain of the "data lifecycle" – in other words, from collection to processing (including all intermediate steps, sub-service providers or data brokers) to archiving and deletion.

### 1.3.6 Information obligations

The data subject has to be informed comprehensively, in writing or electronically, about to what extent and for which purpose personal data is collected. It is differentiated here whether or not data is collected from the data subject themselves. The requirements are extensive and will be challenging to implement, especially given that the information must comply with the transparency requirements (see above). Also in employment relationships, special attention should be paid when preparing for the GDPR in order to document sufficient information with regard to the data subject.

### 1.3.7 Data subject's disclosure rights

Data subjects are entitled to ask the responsible party for confirmation of whether and to what extent the personal data is processed that they provided themselves. The disclosure claim is based on, among other things, the data categories, the processing purpose, the recipient and the duration of the storage. The interested data subject can continue to exercise their right of rectification, deletion, limitation or even their right to objection to the processing. It should be noted that the disclosure right pursuant to Article 15 GDPR in accordance with § 34 para. 1 No. 2 a) and b) of the (new) German Federal Data Protection Act (BDSG) does not exist if data is only stored because it cannot be deleted due to legal or statutory retention regulations or if it exclusively serves the purposes of data backup or data protection control

and the provision of information would require a disproportionate effort and processing for other purposes using suitable technical and organizational measures is not possible.

### 1.3.8 Data portability

In principle, a data subject's provided data must be handed over by the responsible party on request in a common format, which makes a direct transfer from one responsible party to another responsible party technically possible. The claim is limited to data "provided" by the data subject. In the case of a narrow interpretation, only that data which has been actively and knowingly made available by the data subject can be included. The transmission to the data subject or a new responsible party must be unhindered and generally free of charge. In the case of the right of direct transmission from responsible party to another, this is limited to what is technically feasible pursuant to Article 20 para. 2 GDPR.

### 1.3.9 Right of objection

If the data processing of the data subject is based on the safeguarding of public interest or a weighing of interests, they can object to this processing. An explicit indication of the right of objection must be made clearly and separate from other information with the first communication at the latest. The right of objection also applies to direct advertising.

### 1.3.10 Coupling prohibition & appropriation

Additional contractual services may not be linked to the fact that the data subject consents to the processing of the data. Article 7 para. 4 GDPR regulates that consents are only valid if the performance of a contract is independent of the consent to processing that is not necessary for the contractual purpose. However, it should be noted that, in addition to consent, a weighing of interests according to Article 6 para. 1 f GDPR can also be the basis for the admissibility of advertising. Such a perspective makes possible the recitals in which express mention is made of the fact that personal data processing for direct advertising can be considered as a form of processing that serves a legitimate interest.

A particular challenge also exists regarding the documentable appropriation of data processing pursuant to the GDPR for big data applications.

### 1.3.11 Data protection "by design" and "by default"

Data protection principles must be taken into account as early as the product development and implementation phases, meaning that, for example, the data reduction, data minimization and appropriation of the process must already have an influence here. Standard settings in systems, processes or websites are to be created in such a way that the only data required for the specific purpose is collected ("privacy by design/privacy by default"). The legislature also aims to drive the development of new technological design possibilities.

### 1.3.12 Reporting of data breaches

The responsible party must document all data breaches and their effects as well as any remedial measures in a comprehensible manner. Depending on what risk the data breach presents to the rights and freedoms of natural persons, further obligations ensue. If a risk for the data subjects is unlikely, there is no reporting obligation. If the existence of a risk is confirmed, data breaches must be reported to the supervisory authority within 72 hours of discovery. If there is a high risk to the personal rights and freedoms of the data subject, the data subject must also be informed. Here, too, exceptions may be applied to the notification of data subjects, for example, when appropriate technical and organizational safety precautions have been taken.

### 1.3.13 Right to be forgotten

The data subject has the right to data deletion as soon as the storage is not (or no longer) required for compelling legal or contractual reasons. Responsible parties who make personal data available to the public must also inform all third parties that the data subject has requested the deletion of all links or copies/ duplications. Legal retention periods are not affected by the claim for deletion. If a data subject revokes their consent and requests the deletion of their data, the question arises as to whether the proof of consent must also be deleted.

### 1.3.14 Profiling

Data subjects are entitled to not be the subject of a decision based exclusively on automated processing which has legal effect (for example, scoring), unless a dedicated standardized exception exists.

### 1.3.15 Privacy impact assessment

In the case of processing operations that are likely to entail a high risk for the rights and freedoms of natural persons, in future the responsible party must carry out a privacy impact assessment for the purpose of evaluating the cause, type, specificity and severity of the risk of processing. The supervisory authorities may publish positive and negative lists specifying the procedures for which an impact assessment is to be carried out. If necessary, the implementation of the processing must be coordinated with the data protection authority in advance.

### 1.3.16 Data protection organization

Article 24 GDPR refers to a company's organizational obligations in the sense of a plan-do-check-act process. Therefore data protection management must be established within the company organization. Supervision is carried out via existing or newly introduced systems (e.g. internal control system – ICS, compliance organization). External supervision is carried out by the supervisory authority or by auditors and even by the data subjects themselves (e.g. with disclosure/rectification requests). The data protection officer is mainly responsible for the advisory function, as he/she is involved in the planning and risk-based monitoring.

### 1.3.17 Data security

The categorization and structure of the requirements for the obligation to comply with appropriate technical and organizational measures for the protection of personal data deviate from the existing German Federal Data Protection Act (BDSG). This means that companies must check already existing technical organizational measures. When determining security measures pursuant to the GDPR before the start of processing, the specific protection needs must be determined, the risk must be assessed and a proportionate measure must be taken the necessary proof of this (documentation) must be provided. Above all, the confidentiality, integrity, availability and resilience of the processing systems must be taken into account. Those organizations who can rely on an already established ISMS or an existing ISO 27001 certification, as Arvato Systems does, will find it easier to implement these requirements, since systematics and documentation are already known and implemented.

### 1.3.18 Record of processing activities

In contrast to the requirements of the German Federal Data Protection Act, (BDSG) the GDPR does not stipulate a public procedure record. However, a record of processing activities must be drawn up and submitted to the supervisory authority on request. In contrast to the previously familiar procedure record, Article 30 of the GDPR introduces new requirements with regard to the record. In addition, there is now also an obligation for the processor to keep a record of the processing activities it has carried out.

### 1.3.19 Contractor data processing

The previous “contracted data processor” simply becomes the contracted processor under the GDPR. Until now, contracts for the regulation of data processing between the responsible party and the contracted processor have also been necessary. In the future, however, these will no longer have to be in writing, as an electronic format is sufficient. Therefore, the text form (e.g., per click or per e-Signing, the variant preferred by Arvato Systems using the DocuSign® tool) is sufficient. In addition to this easing of the formal requirement, the amendments to the GDPR and the (new) German Federal Data Protection Act (BDSG) require contract adjustments (e.g. reporting data breaches, data portability, issuance and documentation of directives).

In the event of contractual transfer of data processing, the responsible party may, pursuant to Article 28 para. 1 of the GDPR, only contract processors who provide sufficient “guarantees” that appropriate technical and organizational measures are implemented. These “guarantees” can also be demonstrated by certifications or approved rules of conduct. Since the rules of liability also recognize a scale of encumbrance, these guarantees are more likely to be “warranties” in a legal sense to which due diligence is attached.

### 1.3.20 Certifications/rules of conduct

Associations can establish rules for sector-specific data processing and have them approved by the supervisory authorities so that certifications are supported by the GDPR. At this time, no such approvals have been made.

### 1.3.21 Data protection officer

According to the GDPR, a company data protection officer is to be designated only for companies whose core business is data processing that poses particular risks for data subjects. This is a new requirement for some EU countries. According to Article 37 para. 2 of the GDPR, the appointment of a group data protection officer is possible; the data protection officer’s contact details must be published and communicated to the supervisory authority.

In Germany, an order obligation for data protection officers according to § 4f para. 1 p. 4 of the German Federal Data Protection Act (BDSG) already existed. With § 38 of the (new) German Federal Data Protection Act (BDSG), the federal legislature has made use of the already existing possibility for a national provision in Article 34 (4) GDPR. As in the old regulation, companies are still obliged to appoint 10 or more people who will constantly deal with automated data processing. Irrespective of the number of people involved in the processing, a data protection officer must be designated if the responsible party or the contracted processor carries out processing that is subject to a privacy impact assessment.

### 1.3.22 Transmission to third countries, e.g. USA

When transmitting to third countries for processing, the provisions of Article 44 ff. and Article 28 of the GDPR must be observed in particular. The transmission of personal data to third countries (in particular to countries outside the EU) is possible provided that there is an “appropriate level of protection”. International data transfer under the GDPR must be secured by means of the Commission's adequacy decisions, binding corporate data protection provisions or standard data protection clauses (e.g. in contractor data processing contracts or EU model clauses or individual contract clauses). In the absence of new model clauses defined by the EU Commission, the previously used EU model clauses will remain relevant for companies. The existence of the data subject’s express consent or the basis of statutory authorizations (e.g. flight passenger data) are two important exceptions that allow transmission even without an adequacy decision or sufficient guarantees from the receiver.

### 1.3.23 European Data Protection Board/coherence obligation

The EU member states must set up independent supervisory authorities; these, however, must co-operate with the EU Commission for the uniform application of the GDPR. One representative from the national authorities is appointed to the “European Data Protection Board”. According to § 17 of the (new) German Federal Data Protection Act (BDSG), this is the Federal Commissioner. The GDPR contains essential provisions for the co-operation and coordination of national supervisory authorities and cross-border circumstances; these are intended to serve the uniform application of the GDPR.

### 1.3.24 Right of association

Also new is that consumer protection associations are able to initiate proceedings for the violation of data protection regulations. They are also given powers to assert claims for damages on behalf of data subjects, if the association was commissioned on their behalf. The circle of claimants is extended particularly in the area of B2C data processing.

### 1.3.25 Liability

Alongside the responsible party, the contracted processor will be equally liable to the data subject for compensation (but only within the context of its contractual duties and responsibilities). This means that companies may also be obliged to compensate data subjects for non-material damage. As already mentioned, in addition to the responsible party and contracted processor’s expanded joint and several liability, the fine amounts of up to 20 Million EUR or 4% of a group company’s total global turnover have also been amended.

## 2 Arvato Systems Group and implementation of the GDPR

How have the companies of the Arvato Systems Group prepared themselves for the implementation of the GDPR?

As a proven IT expert in the Bertelsmann Group, we have already committed ourselves to an early-stage enterprise work group, which comprehensively deals with the General Data Protection Regulation. Data protection experts from the various Bertelsmann divisions are engaging in an intensive dialogue, educating themselves at conferences and thus provide an up-to-date and comprehensive knowledge of everything to do with the GDPR. And this knowledge was the basis for very specific measures.

A new Bertelsmann management guideline for data protection, which is clearly coordinated with the GDPR, was adopted in early 2017. Fundamental contract documents – for example regarding order data processing – were adapted accordingly. In addition, we have created and placed the requirements for the introduction of necessary future procedures throughout the Group online. Whether processing records or data protection reports – we use synergies and reduce the existing degree of complexity for documentation obligations.

Arvato Systems is very well positioned in terms of privacy issues. Therefore, new necessary measures concerning the GDPR could often be integrated into existing processes and documentation. Some examples:

- Arvato Systems has long used an information security management system (ISMS), which is derived from ISO/IEC 27001.
- The operation of our data centers in Gütersloh and Leipzig is certified according to ISO/IEC 27001. Both data centers operate internal control systems which are audited by KPMG within the framework of an ISAE 3402 Type II report.
- The reporting process for security incident management has long been established and could be expanded to the meet the requirements of the GDPR.

- Our existing electronic document management system serves as a basis for contractual documentation obligations.
- Arvato Systems use E-Signing across the Group. This significantly expands the digitization of contracts and the resilience of document management.
- Overall, internal control systems (ICS) at Arvato Systems have long been standard and established as a key for a risk-conscious corporate management. The corresponding processes are based on plan-do-act-check cycles.

In order to provide the best possible support for our specialist areas, we have also strengthened our staff, continually expanded our in-house data protection expertise and were certified for the GDPR by the German Society for Data Protection and Data Security (GDD). After initially using the expertise of external specialists, for example for detailed gap analyses, to gain additional valuable insights through an additional view of processes, we are now working in data protection management in a continuous PDCA cycle. Of course, this is always done together with the responsible parties in the relevant departments and with active support from the management

Our strengths include the continuous expansion of expertise, intensive cooperation with experts concerning specific questions, extensive engagement with a wide range of aspects relating to the GDPR in the Group context as well as to Arvato Systems itself and clear implementation expertise. We use our experience and knowledge daily for our own company.

All of this is what makes our team stand out.