GDPR for Database Developers

Version 1.0.2 from 27th January 2020

Content and objectives

This whitepaper provides IT professionals and especially database developers with essential information and instructions on the GDPR in a concentrated form and understandable language. From the mass of legal texts, books, websites and articles on the GDPR, data protection and data security, we filter out what the practitioner actually needs to know, understand and implement.

The technical implementation using Microsoft Access and Microsoft SQL Server is covered in separate sections. The further contents do not refer to specific database systems, because the requirements are the same for all.

Our approach to data protection is our own professional practice as independent developers and IT specialists. In addition to findings from seminars, lectures and discussions, experience gained from our consulting activities and practical implementation for customers is also incorporated.

We are not lawyers. This whitepaper represents our views and opinions on the subject and is not legal advice.

Authors

Karl Donaubauer, Vienna

web: donkarl.com, contact: office@donkarl.com
database developer, MVP for Microsoft Access
Certified Data Protection Officer

Lectures on the GDPR in at, de and the USA. Consulting and practical implementation of the GDPR requirements for customers and developer colleagues in at and de.

My position on the GDPR:
Pragmatic and positive. Conscious, proactive handling of the subject and comprehensibility are closer to the spirit of the regulation than the pseudo-judicial approach of trying to protect oneself against everything and everyone with many (often inappropriately and thoughtlessly copied) texts and formalisms.

Bernd Jungbluth, Horn

web: www.berndjungbluth.de, contact: info@berndjungbluth.de
consultant, trainer and database developer for, with and in Access and SQL Server
Certified Data Protection Officer (TÜV), graduate business economist

Lectures and seminars on data protection and data security with Access and SQL Server
Both topics play a central role in my consulting, trainings and database development work.

My attitude to data protection
I see data protection as an elementary component of data processing. I am particularly interested in the technical aspect - and that goes beyond the processing of personal data. Starting with data protection, I focus on data security and IT security in companies.

Philipp Stiefel, Hofheim am Taunus

web: https://codekabinett.com, contact: phil@codekabinett.com
Software developer and process consultant

Contact with GDPR:
Software development and consulting on application and data security in the conflict between government supervision and regulation (financial services) and the protection of personal data.

My attitude to data protection:
The GDPR has finally enforced adequate attention to the handling of data both at the persons concerned and the responsible companies. Blind, formal-juridical actionism without a differentiated examination of the subject are counterproductive excesses.

Table of contents

Roles and Terms

The GDPR uses some defined and established terms. In this section we explain the terms that are essential for understanding the content of this paper.

Personal data

„any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"
- Definition acc. to article 4.1. GDPR

Special categories

Some of this information is particularly worth protecting. In Article 9 of the GDPR, these are referred to as "special category" data and include data on racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, data on sex life or sexual orientation.

Data subject

According to the GDPR, every person whose personal data are stored and processed is a data subject. This includes, among others, the company's own employees and the contact persons at customers, suppliers and business partners.

Data processing

" any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;"
- Definition acc. to article 4.2. GDPR

Or from the point of view of the database developer: Everything you can do with data.

Controller

The central role in data protection is the controller. He is the natural or legal person who determines the purposes and means of the processing of personal data. The controller has extensive tasks and duties, which we explain in this document.

Processor

The processor is a natural or legal person who processes personal data on behalf of the controller. He has similar tasks and duties to fulfil.

Data Protection Officer

The tasks of the data protection officer are the conceptual consultation of the controller and the training of the employees. As a rule, he draws up the data protection concept and monitors its compliance, but

is not personally responsible for its implementation and execution. He is also the contact person for data subjects and the supervisory authority.

The data protection officer can be an internal employee or an external service provider.

We describe the requirements for the appointment of a data protection officer in the section "Data Protection Officer".

Technical and organisational measures

All activities and arrangements that ensure the secure processing of personal data are summarised under the term "Technical and Organisational Measures" (TOMs). We describe them in more detail in the section of the same name.

Principles of processing

The processing of personal data must comply with the principles defined in article 5 of the GDPR:

- lawfulness, fairness, transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality
- accountability

These principles are fundamental for GDPR-compliant data processing. In particular, we would like to highlight the lawfulness and purpose limitation. The other principles are no less relevant and are incorporated into the text at the appropriate places.

Lawfulness

Processing is lawful only if the data subject has given his consent, if it is carried out in order to fulfil a contract or to carry out pre-contractual measures (offer, order confirmation etc.), if there is a legal obligation, for the protection of vital interests or for the performance of tasks in the public interest.

A special exception is the protection of the legitimate interests of the controller. The interests of the data controller and those of the data subject must be weighed against each other.

Purpose limitation

Personal data may only be collected for a clear and specified purpose. Further processing for another purpose is only permitted if it is compatible with the original purpose.

Company-wide tasks

The practical implementation takes place in several steps. It starts with an inventory. This shows the scope of the tasks and duties, from which the technical and organisational measures for implementation result.

Inventory

An inventory can be very different. Your own position and point of view play a decisive role here:

- Independent database developer as entrepreneur
  Responsible (controller) for his own IT and datasets and thus for the implementation of the GDPR in his company
- Independent database developer as contractor
  with projects such as the creation of database applications and specifications, performance optimisation, consulting etc.
- IT employee
  administrator, database developer etc.
- Employee in the role of data protection coordinator

It is worth taking the perspectives of other roles as well as one's own when taking stock. It is important to involve all relevant persons - from the management to the department heads to individual employees. The form is completely free. It can be a Word document, an Excel spreadsheet, or an own Access database.

We cannot provide a general template for an inventory at this point, but we do provide a checklist in the appendix.

Tasks and duties

The GDPR imposes obligations with primary external effects. Since their fulfillment or nonfulfillment is easy to recognize from the outside, they should be addressed first. After this the tasks are to be done which are predominantly directed inwards.

As already mentioned, many activities are interlinked in practice. A sharp separation is not possible. We are concerned here with the tendency from the outside to the inside, which we therefore follow in the listing and description of duties.

Information duties

Every person should know who collects and processes which data about them. This is the key point in the most important principle of the GDPR: fair and transparent processing. For this reason, the data subject shall be informed of the following points when collecting their data:

- Contact details of the data controller
- Contact details of the data protection officer
- Purpose of data collection
- Lawful basis
- Storage period
- Rights of the data subject
- If applicable, transfer of the data to third parties or to non-EU countries

Articles 13 and 14 of the GDPR list about 1 dozen further points that must be included in the information, e.g. the reference to the right of objection, especially in the case of direct marketing.

Controversial is the way in which the information is transmitted. Some describe the processing of the data in a document that is handed over or sent to the individual at the time of data collection, most link or refer to the privacy statement of their website or provide a short text as a footnote in e-mails and letters.

Privacy statement

It includes all points from the information duties and belongs to the website. This applies in particular when personal data is collected there via contact forms. But even without this obvious collection of data, it is still relevant, since the IP addresses of the visitors are stored when the website is accessed, possibly the surfing behaviour on the website is analysed using tracking tools such as Google Analytics, and much more.

There are many templates for data protection declarations - on the Internet with the supervisory authorities, with the competent chambers and with external consultants. Wherever the template comes from, almost always it must be adapted to one's own reality.

Example:
The employee responsible for the corporate website had copied the privacy statement from a WordPress template. Among other things, a detailed description of the handling of personal data from the contact form and blog comments. When asked where the contact form and the blog were, he had to fold. Both were not available on the website.

Such a privacy statement will signal to users of the website that the privacy practices of that company are only considered a chore.

We have reviewed the data protection declaration and adjusted it for all irrelevant points. After that it was clear, credible and only half as long.

Websites and GDPR are an important and comprehensive topic and should be reviewed and adapted with respect to the GDPR. There are many points to consider, such as newsletters, contact forms, embedded content such as the Google character set „Font Awesome“ and social media plug-ins.

This topic is too extensive to be dealt with exhaustively at this point. Therefore we refer to an article of the IHK Munich: https://www.ihk-muenchen.de/dsgvo-datenschutz-webseite/ (website in German)

Reporting obligations for data breaches

The handling of data protection violations is regulated in articles 33 and 34 of the GDPR.

- If there is a risk for the data subjects, personal data breaches must be reported to the supervisory authority.
- The notification must be made within 72 hours.
- If a personal data breach is likely to result in a high risk to the data subjects, they must also be informed of the breach and its potential consequences.
- Such notification must be made immediately („without undue delay“).

The organisational structures and scenarios of companies differ greatly. Therefore, the flow of information and the policy for dealing with data breaches vary. In order to be able to act quickly and effectively in the event of a data glitch, it is necessary to draw up an action plan in advance for one's own situation.

The basic prerequisite is employee training. They should recognize data breaches. Unrecognized privacy breaches can neither be reported nor countermeasures taken.

Rights of data subjects

The data subjects may claim extensive rights in accordance with GDPR art. 15 to 22. In this case, the data controller should be prepared, as the fulfilment of the individual rights is associated with an effort that should not be underestimated. Although this can be reduced by organisational measures, there is no standard recommendation for this due to the wide variety of scenarios.

Hint:
Irrespective of the right claimed, the identity of the inquirer must always be ensured. To this end, an appropriate identity verification procedure shall be established. If the data of a wrong person are supplied, deleted or changed, this is a privacy breach.

- Right of access
  - Confirmation of the processing of the data, including information on the purpose of processing, categories of data processed, storage period, recipients, origin etc.
  - Copy of personal data
- Right to rectification and completion
  - Correct wrong information
  - Complete data that is incomplete for the purpose of processing
- Right to erasure
  - In principle, deletion must be carried out immediately.
  - In consideration of exceptions such as legal storage obligations, pending legal disputes, public interest etc.
- Right to restriction of processing
  - Lock data against further processing
  - Protect data from deletion - restriction applies only temporarily until the clarification of open issues such as disputed accuracy of data, clarification of legal disputes etc.
- Right to data portability
  - Data transmission to the data subject or directly to another controller
  - In a standard machine-readable format
- Right to object
  - Stop data processing
  - For direct advertising always and without special reasons
  - For other processing with individual reasons
- Right to individual assessment of automated decisions
  - Have a natural person review and evaluate the decision
  - Applies to processing with legal effect, such as profiling etc. and only under certain conditions

If the controller does not fulfil the rights of a data subject, he or she may complain to the supervisory authority. The controller must inform about this right of complaint.

Time limits (GDPR art. 12.3)
Upon receipt of an application, the controller must react immediately. The data subject must be informed within one month of the stored data or the measures taken (deletion, correction, limitation etc.). In particularly complex cases, this period can be extended by a further 2 months with good justification. The applicant must be notified of this extension and its reasons.

Data processing agreement

The processor is a natural or legal person who processes personal data on behalf of the controller. He is subject to the instructions of the controller and implements the agreed procedure.

The instructions as well as the agreed TOMs are to be recorded in writing in a data processing agreement/contract. This can also be done in electronic form. The initiative is taken by the client/controller.

The contract must state that the processor must provide the controller with proof of compliance with the contract and enable him inspections, that the data have to be returned or deleted after the end of the processing activity, and much more. The exact contents of the contract are regulated in article 28 GDPR. Templates for contracts can be found at supervisory authorities, chambers and associations.

After the initial check, the contracts should be checked regularly for their up-to-dateness and correctness as well as their implementation and compliance. This applies to the controller as well as to the processor.

In our experience, there is often no written contract, even if it is a clear case of order processing. On this point, the GDPR has not yet arrived everywhere in economic life, and in many cases there is still a need for clarification and action. However, the contract is helpful in defining the roles and duties in the handling of personal data.

In practice, it is not always clear whether you are a processor or have different role. Let's take a software developer. If he uses only test data and does not have access to the real data, he is not considered a processor and therefore no processing agreement is necessary. Whereas an external network administrator can be a processor. He administrates the productive systems and thus has access to data carriers and files with personal data.

Also not trivial is the demarcation between a processor and an independent controller. For example, tax consultants and lawyers are not regarded as processors because they are not bound by instructions in the performance of their duties.

Record of processing activities

The record of processing activities contains all processing activities with personal data in a company. It must be carried out by each controller to whom one of the following points applies.

- The company has 250 or more employees.
- The processing involves a potential risk for the data subjects.
- The processing is „*not occasional*“.
- Data of special categories are collected.

The record does not have to be a mere formal act, but in practice is the starting point for many companies to research and deal with personal data. A well-maintained processing record is the central document for the administration of relevant activities and provides the necessary overview. It can be used as a guide for the periodic inspection of existing processing activities and as a model for the introduction of new processing operations. Therefore, a processing directory is also recommended in cases where it is not prescribed.

Our sample document in the appendix shows an excerpt of a typical example of a processing record.

At the request of a supervisory authority, the record of processing activities and associated documents (list of TOMs, IT security concept etc.) must be submitted. Contrary to the old BDSG

(Bundesdatenschutzgesetz = German Federal Data Protection Act), the records no longer have to be published.

A processor must also keep a record of processing activities for each client/controller. In addition, the name and contact details of the client/controller must be included. On the other hand, the following points are not necessary:

- Purposes of processing
- Categories of data and subjects
- Categories of recipients
- Time limits for erasure

Data protection impact assessment

According to Article 35 of the GDPR, any processing of personal data shall be subject to an assessment of the risk that data subjects may be exposed to as a result of data breaches or abuses. The risk assessment or threshold analysis is an informal process that clarifies the need for a data protection impact assessment for a processing operation. Documentation of the risk assessment is not required under the GDPR, but in Germany it is required by the data protection authorities, including an indication of the main reasons.

If the examination reveals a potentially high risk, a data protection impact assessment must be carried out. Based on the risk determined and the probability of a data breach occurring, suitable TOMs are now to be defined with which the risk and probability of occurrence can be reduced. The measures will be subjected to a new analysis and evaluation. If there is still a potential high risk, the data protection authority must be consulted.

There are some guidelines and tools for data protection impact assessment. For example, the supervisory authorities publish black- and whitelists that list processing activities that may or may not require a DSFA. Furthermore, the French national data protection authority (CNIL) offers the PIA tool (PIA = Privacy Impact Assessment) to create a data protection impact assessment: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

Further information on the data protection impact assessment can be obtained from the Bavarian State Office for Data Protection Supervision: https://www.lda.bayern.de/de/thema_dsfa.html (website in German)

Data protection officer

The tasks of a data protection officer (DPO) include neither the implementation of the GDPR nor the implementation of the TOMs. He monitors data protection compliance in the company, advises and trains employees and cooperates with the supervisory authority.

For these tasks he must have expertise in the field of data protection law. There is currently no formally binding qualification or even certification for a data protection officer.

According to the rules of the GDPR, controllers and processors must appoint a data protection officer in the following cases:

- At public authorities
- Core activities include extensive, regular and systematic monitoring of persons
- Core activities include processing on a large scale of data of special categories or data relevant to criminal law

In addition to these rules, in Germany there are other reasons for appointing a data protection officer. These are defined in § 38 BDSG. The two most important are:

- A data protection impact assessment is required.
- At least 20 persons (since autumn 2019) are permanently occupied with the automated processing of personal data.

The contact details of the data protection officer must be published and communicated to the supervisory authority.

The data protection coordinator/manager

A data protection coordinator or data protection manager practically implements the requirements of data protection in a company. Although this role is not defined in the GDPR, it is common in practice.

This is often an IT employee, as he has technical knowledge of IT and databases and is familiar with the company's data processing operations. In addition to numerous internal tasks, his practical work sometimes even includes the preparation and assessment of GDPR-compliant cooperation with external service providers and software suppliers.

For these additional tasks there is often neither a budget worth mentioning nor a corresponding training - and this although the employee not only takes over the tasks of the controller, but often also those of the data protection officer.

Data protection adviser

In addition to the data protection officer and the data protection coordinator, there is a third role, the data protection adviser. Companies with a lack of data protection know-how can turn to such an external expert. In addition to basic advice, he can be consulted on an ongoing basis to assess new situations, technical possibilities and data.

Considering the number of companies that do not need to appoint a data protection officer and the complexity of the requirements, the data protection adviser is becoming increasingly important. Maybe in a few years he will be as natural as a tax adviser.

Data security

Data protection is the protection of rights of natural persons. The technical and organisational protection of data, on the other hand, is summarised under the term "data security". It goes beyond the personal data and concerns all data of the company.

The GDPR refers to data security in article 25 "Data protection by design and by default". At this point we quote from article 25.1:

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures[…].

"Data protection by design" refers not only to the processing of data, but also to the planning, procurement and design of new products and services. The legislator demands therefore already with the procurement of a new software, like an ERP or CRM system, that it corresponds to the principles of data security. On the other hand, manufacturers are required to equip their software and services with appropriate features and security measures.

"Data protection by default" expects the most privacy-friendly configuration of the systems as the default configuration. Available security mechanisms should always be enabled unless they are disabled by a deliberate and well-founded user action. This refers to the amount of data collected, the extent of their processing, their retention period and their accessibility.

This scheme is aimed primarily at large companies, such as Facebook and Google, which earn their money by analysing and trading data. These data vampires have reacted since the GDPR came into force and adjusted the default settings of their systems. Of course, this principle applies to all developers and providers of applications with which data is processed.

Example: In an Access application, developer functions such as navigation pane, ribbon, shift key etc. are deactivated for all users.

The second article dealing with data security is article 32 "Security of processing". This specifies the implementation of data security and requires an analysis of the necessary level of protection.

The classification of protection needs is a recurring process. Any new project or change in the data categories used in the project will require a reassessment of the level of protection of the data concerned.

Example: In an existing project, a database developer receives an additional table from the customer containing health data. In the GDPR, health data fall under the so-called "special categories" and require a high level of protection. Therefore, the level of protection needs to be re-evaluated and probably increased.

The IHK Munich offers assistance in determining the appropriate level of protection: https://www.ihk-muenchen.de/de/Service/Recht-und-Steuern/Datenschutz/Die-EU-Datenschutz-Grundverordnung/Datensicherheit/ (website in German)

The GDPR lists the following technical and organisational measures to ensure the safety of processing.

- Encryption
- Pseudonymisation
- Ensure the confidentiality and integrity of systems and services
- Ensure the availability and resilience of systems and services
- Enable rapid recovery of systems and services
- Check and evaluate the effectiveness of the measures

Technical and Organisational Measures (TOMs)

The GDPR defines technical and organisational measures (TOMs) as measures within the framework of an IT security concept as well as within the framework of technical protection of personal data in files and databases.

Whereas in the GDPR the TOMs are only described in abstract terms, the German Federal Data Protection Act (Bundesdatenschutzgesetz, abbr. BDSG) is more concrete and specifies the following points in detail as TOMs in Section 64 (3). According to the BDSG, these points apply to police and justice, but they are also useful for companies. We take over the points and supplement them with explanatory keywords.

- Access control
  Physical access to the IT infrastructure, such as security doors, locking and alarm systems

- Data media control
  Prevent unauthorised access to data carriers, USB flash drives, hard disks, mobile devices etc. through measures such as encryption and proper deletion by document shredders with crosscut and correct hard disk destruction
- Transmission control, transport control
  Secure and possibly encrypted transmission to external interfaces such as web services, FTP server, VPN etc.
- Storage control, user control, access control
  Access only for authenticated users to systems and data in their area of responsibility through password management, smart cards, firewall etc., or something as lapidary as locking computers when absent ([Win]+[L])
- Input control
  Traceability of the entry, modification and deletion of data
- Reliability, data integrity, availability control
  Fast detection of malfunctions, UPS, fire detectors, anti-virus software
  Patch management for hardware, routers, mobile devices, operating systems, applications, websites, telephone systems, printers etc.
- Recoverability
  spatially separated and regularly checked backups, supplemented by a disaster recovery strategy
- Order control
  Control of processors and contracts
- Separability
  Ensure separate processing of personal data collected for different purposes

Hint:
A purely organisational and nevertheless one of the most important measures is the sensitisation and training of employees. Uninformed employees annul most technical safety precautions - consciously or unconsciously.

Many of the TOMs mentioned should already have been implemented within the framework of an existing IT security concept. The GDPR only adds a few new aspects here. Examples of IT security concepts are available from the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, abbr. BSI): https://www.bsi.bund.de/EN

Data protection compliant software development

The scope of software development ranges from formulas that an employee enters in an Excel sheet to the creation of individual or standard software by an external service provider. The principles of data protection must be observed everywhere in this broad spectrum.

Many official recommendations for action such as those of the BSI refer to the creation of software by an external service provider. The situation of an internal developer is usually not dealt with. In both cases, the software development process should be coordinated with the controller and, if applicable, the data protection officer.

Data for requirement analysis / concept development

Even before the actual start of the development work, the developer often receives real personal data for the requirements analysis and offer preparation of existing customers or even interested parties.

This is critical for data protection reasons. On the one hand, the developer is now also responsible for the security of the data, on the other hand, the principle of purpose limitation is contradicted, since the sender has certainly not collected the data for the purpose of software development by a third party. In addition, there is no corresponding data processing agreement.

Even if data processing agreement already exists, it must first be checked whether the technical and organisational measures in the contract are sufficient for the newly received data.

We recommend a prompt consultation with the sender of the data in order to clarify the further and above all data protection-compliant processing. The following scenarios and procedures are conceivable:

- Requirements analysis without personal data
  with anonymised data, with fictitious test data or without data based on the structure
- Requirements analysis at the customer's site
- Discuss requirements with the customer via remote maintenance

Hint:
Personal data transferred in paper form must also be treated in accordance with the data protection rules. Among other things, they must be stored safely and returned or properly disposed of when the project is completed.

Data in development

The further development of software, as well as troubleshooting directly in the productive environment comes with increased risk. Data can be falsified or deleted by errors of the developer and by unfinished software. For this reason, software development should not take place in the productive environment.

The risk of unintentional modification or deletion can be eliminated by using a copy of the data in a test environment to develop the software.

This environment for development and testing must be sufficiently isolated in order not to cause any falsifying changes in the productive environment, e.g. delete files, create PDFs in the invoice folder,

exports to interfaces. To set up an isolated test environment it is usually necessary to create separate folders for imports, exports and interfaces and to enter these in the configuration of the test environment accordingly.

In terms of data protection law, it does not matter whether the processed data is directly available in the live system or as a copy. As soon as real personal data is used, this data, the development process and the development environment are subject to the requirements of the GDPR. This of course includes the security of the processing, such as the encrypted storage and transfer of data, as well as the safe storage of storage media (e.g. USB sticks) and backups. Many data breaches occurred with copies of real data in development environments.

Example:
An insurance company has superbly secured its productive environment and virtually ruled out unauthorised access to it. However, the internal software development worked with a copy of this data. This copy was the easy target of attackers because the security measures used there were insufficient.

Artificial test data, on the other hand, are not subject to the GDPR. They are therefore preferable to a copy of the real data. This applies to sensitive data in particular and the transfer of data to external developers. However, the use of real data cannot always be avoided, e.g. for the analysis of data-dependent errors.

With some effort test data can be generated with own routines, whereby these are closer to the requirements of the project. Alternatively, there are commercial tools for generating test data.

Hint:
Personal data can also be found in processes related to software development. This includes error messages that are sent to the developers as screen shots or stored in ticket systems, traces for performance optimisation, and so on.

Database applications

The aim and purpose of a database application is to process and store data. As in most cases personal data are included, the GDPR also applies to the development of such applications. This results in some new requirements for database development.

The developer needs functional support from the client or his data protection officer or data protection consultant for this. He alone cannot assess which data are absolutely necessary, how they are to be handled and what level of protection they require.

Classify data

To be able to quickly localise personal data in a database if required, it is advisable to classify the data columns of all tables. A distinction should be made between simple and special personal data. There are many reasons for such a localisation: the fulfilment of the obligation to provide information, the correction of incorrect data, the deletion of data after fulfilment of the purpose or on request etc.

Ensuring integrity

Integrity refers, among other things, to the processing of correct data. The consistency of the data can be achieved in databases through the functions of declarative integrity, such as foreign key relationships, unique keys etc., a procedural check of data integrity through programming in VBA, T-SQL or similar.

Logging changes

New entries and changes to personal data must be logged with date and user name. In addition, the values before and after the change can be recorded in the log.

The purpose of logging is not only traceability. The logged modification date can also be used to determine the data whose retention periods have expired.

Minimising data

The principle of data minimisation is already to be considered when designing the data model. It should only include data that is relevant to the business processes of the application.

Data already collected which were not necessary for the fulfilment of the purpose shall be deleted in accordance with the provisions of the GDPR. Common suspects: date of birth, sex, private mobile phone numbers etc.

Deleting data

Once the processing purpose has been achieved or if the legal basis does not exist (any more) - in practice often after the expiry of legal retention periods - the data must be deleted or anonymised. Data must also be deleted at the legitimate request of the data subject, as must incorrect data that cannot be corrected.

For all personal data, deletion times must be specified. The starting point for this can be the above-mentioned modification date or, for example, an invoice date. This defined date also serves to prevent the deletion of data records that may not yet be deleted.

For this purpose, a suitable functionality must be provided or supplemented in the application in order to enable deletion while checking the retention periods and any lock flag.

Anonymising data

An alternative to deleting data is anonymising it. Anonymising means that the data cannot be assigned to specific persons and that this assignment cannot be restored.

Anonymous data is not covered by the GDPR.

Anonymisation can be used to use the data for statistical purposes and tests with data sets even after expiration of the deletion periods.

Ensuring confidentiality

In order to meet the requirements for confidentiality, e.g. through multi-client capability, functional separation or visibility of data, the database model must enable graded access authorisations.

Employees should only be able to access data that is required for their tasks. Examples would be access authorisation at department level, branch level or multi-client capability.

Of course, the implementation depends on the requirements and the technical possibilities of the development tools. The spectrum ranges from the physical separation of the data to the design of the user interface.

Pseudonymisation of data

With pseudonymisation, the identification features of a person are replaced by identifiers. The assignment of the pseudonymised data to the actual person is possible at any time using the underlying concept or algorithm.

For this reason, the concept and algorithm must be stored separately from the pseudonymised data and protected against unauthorised access by suitable TOMs.

Pseudonymisation is merely a means of increasing the security of processing. The data continue to fall under the GDPR.

Encrypting data

The encryption process is similar to that of pseudonymisation. Again, the original content is replaced by other values, except that the conversion is done by a key. The key turns the plaintext into unreadable gibberish.

> Hint:
> The conversion of encrypted information into readable plaintext is no longer possible without a key. Therefore, the keys used should be carefully managed and secured. This usually amounts to key or certificate management.

Interfaces and external files

Database applications are surrounded by other systems and files, such as imported and exported CSV files, PDFs, emails and paper printouts. Tools such as Word serial letters or Excel pivot charts store a copy of the data independent of the original database. Error logs and other log files may contain personal data. Access rights to external systems are stored legibly in the source code or in configuration files.

In all these examples, the security of the processing must be guaranteed, e.g. by limited access rights or the encryption of the files before data transmission. The purpose limitation must also be taken into account. If it is at all given, the data are to be deleted after reaching the purpose.

The examples show the necessity of a data flow analysis. Here the path of the data into and out of the database is analysed and documented.

Database management systems

The requirements can be implemented with many database management systems. The following chapters cover Microsoft Access and Microsoft SQL Server.

Although Microsoft Azure SQL Databases is closely related to SQL Server, there are some differences, especially in terms of administration and functionality. However, some of the points described in the "SQL Server" chapter also apply there.

The same is true for other database management systems such as Oracle, MySQL and MariaDB. However, terminology and implementation approaches may differ.

Microsoft Access

Microsoft Access is the world market leader in desktop databases and part of the most widely used Office suite. This has implications for data protection.

Access is used by millions of users for a variety of tasks in the small to medium range of databases, from individuals managing private data to corporate data in globally networked corporate departments. Therefore, vast amounts of personal data are stored in Access databases and processed with Access applications. Most Access developers are not part of IT departments, do not have budgets, training or tools for data protection.

If one takes as a measure database management systems in general, some features in Access (or their absence) do not correspond to the "state of the art" required by the GDPR for data protection.

If, on the other hand, desktop database systems are taken as a measure or compared with other desktop programs such as Excel, in which vast amounts of personal data are processed, the assessment is different. These desktop tools have similar data protection mechanisms, but often do not have the advantages of Access: flexible database capabilities, RAD capabilities i.e. easy, fast, efficient programmability, UI creation and customisation.

In case of high data protection requirements, the application (frontend) can remain in Access and the data storage (backend) can take place on a server database system such as Microsoft SQL Server, which offers more and better features for data protection.

The GDPR requires appropriate technical and organisational measures. The appropriateness arises from the risk that the data subjects may be exposed to as a result of the processing of their personal data and from the nature and extent of the processing activities. Our general recommendation is therefore to take all measures that contribute to this adequacy. With Access, these are all the usual measures for securing data, interfaces and designs.

Authorisation at file system level

Since Microsoft Access is a file-based database, only those users should generally have access to the corresponding folders at file system level who actually work with the respective Access application. However, the technical implementation of Access requires that these users, to modify the data, need write and delete privileges to the database file folders so that Access can create and delete the lock file (.ldb/.laccdb).

Deploying Access applications via a Terminal Server

Access applications are often provided via terminal server technology such as Windows Terminal Services, Remote Desktop or Citrix variants. In addition to performance and administration benefits, this also increases the security of file-based applications such as Microsoft Access, as direct access to files via the network can be restricted.

Use database password

Access databases with personal data can be encrypted with a database password. The encryption algorithm has become much more secure with the change of the database format from MDB to ACCDB as of Access 2007. When choosing the password, the usual rules for assigning a secure password must be observed: At least 10 digits, consisting of letters, numbers and special characters. The well-known

crack tools for access files in the ACCDB format work with brute force attacks and are therefore less effective against a long and complex password.

> Hint:
> In practice, the password length for backend files is limited to 19 characters. Longer passwords can be assigned, but from 20 characters on access to linked tables fails with the error message "Not a valid password".

The database password of the backend is held in plain text in the Connect property of tables linked from it and is therefore easy to read. It is therefore important to also encrypt the frontend with a database password to protect already linked tables. In this way the file chain is closed against intrusion attempts.

Disable/hide developer functions

Access offers many functions in its program interface that are intended for application development. The developer should create a secure user interface for the users to prevent access to these functions.

- Hide standard ribbons with developer functions and possibly use custom ribbons instead
- Hide the Navigation Pane
- Disable special keys
    - [F11] for displaying the Navigation Pane
    - [F7] opens the spellchecker dialog, which displays text formatted as password in plain text
    - [CTRL]+[G] opens the VBA editor and shows the Immediate window
    - [ALT]+[F11] opens the VBA editor
    - Shift key for bypassing the startup options and the Autoexec macro

Implement user control

Users can be identified by their Windows login. Usually this is done in VBA with API functions. Individual users can then be assigned an authorisation level/group within the application that grants them access or update rights only to the data, forms and reports and controls required for their tasks.

This form of user control within the Access file only improves the security within the Access application and does not prevent external access to the data via Excel, Access, ODBC etc. For legitimate users of the application this cannot be prevented, for others a restriction of the authorisation on file system level is sufficient.

Use ACCDE format and Runtime version

These Access features limit immediate changes to the application design.

In an ACCDE file, the source code is only available in compiled form and cannot be viewed or modified. Modifying modules, forms and reports is not possible, but macros and especially tables, queries and data are unprotected.

The Access Runtime version hides the navigation pane, the ribbon commands required for design, and hides the design views of the objects. The Access application can only be used with a user interface created by the developer.

These two technical measures do not prevent external access to the data.

Assessment of the possibilities in Access

Some of the measures mentioned so far are not high hurdles for professional attackers, but they are for the large mass of users. They help to limit or regulate the accessibility of the data and designs, thus also helping to avoid errors in data processing.

Classify database and application objects

All parts of databases and applications for the processing of personal data should be classified in order to facilitate and automate their discovery and treatment. Access does not provide built-in tools or features for this purpose. In principle, two methods are possible:

1. Existing features such as the property "Description" of tables, queries, forms and reports are used or misused to store an abbreviation such as "GDPR1", "GDPR5", which represents a label and classification of the sensitivity of the data. Another option is to have dedicated fields in the individual tables for these two tasks. Another variant would be the use of user-defined DAO properties, which are created and filled by VBA programming. All these methods have in common that the GDPR-relevant features are visible and accessible directly on the respective object.
2. A metadata table or database is used to do and store the labelling and classifications of the database objects. This procedure combines all GDPR-relevant information in one central place.

Both procedures allow automated evaluations via VBA or with queries. Separate metadata tables are easier to manage and evaluate. In contrast, classifications that are directly in or on the object are easier to keep up-to-date when changes are made to the object. This information is also not lost when the object is exported or imported into another database.

Log data changes

Logging can be implemented in Access with fields for the changing user and the modification date directly in the respective data-holding table. The advantage of this method is its immediacy. The modification date can be automatically written to the table with the default value Date() or Now(). Access does not offer such a simple solution for the user name. It must be written to the records by programming behind forms.

Another method of making changes traceable is to use a meta-logging table. This again requires programming via VBA. The advantages of this method are the centralisation of the change data and the multi-level nature. All changes can be logged, not just the creation and the last change, as is usual for logging in the data table. For this purpose Thomas Möller offers the ready-made component TM-AenderungsProtokoll:
https://team-moeller.de/?Downloads:TM-AenderungsProtokoll (website in German)

Deletion, anonymisation and minimisation of data

To delete records, you can create a set of delete queries in Access. These delete based on the respective relevant invoice date or last modification date.

As an alternative to deletion, the data can also be anonymised. The anonymisation of data in Access can only be realised by custom concepts and development of custom functions.

It often happens that only parts of the personal data have to be removed as they are no longer used to fulfil the purpose. This data minimisation can be implemented in Access with update queries.

Example:
A customer's payment is converted from credit card to direct debit. The credit card data in the customer master data is no longer necessary and can be deleted.

Document and demonstrate TOMs

Technical and organisational measures must be documented according to GDPR. This is done mainly through formal tools such as the record of processing activities and a catalogue of TOMs. However, it can also be done immediately by naming the above mentioned delete and update queries as appropriate, e.g. qry_GDPR_invoice_data_legal_retention_period_10_years_delete.

In this way not only the GDPR awareness and the TOM character are demonstrated and documented. With a prefix like "qry_GDPR" these queries can also be easily found for regular manual execution or automated.

Prepare fulfilment of rights of data subjects

With Access, the rights listed in the section "Rights of data subjects" can be prepared and fulfilled very well and comfortably.

Let us take the extensive information rights and obligations as an example. The requests of the data subjects and the associated deadlines can be managed in Access. After the personal data has been classified (see above), the answer can be largely automated. The relevant data is determined, displayed in reports and sent by email as a PDF file, for example.

The same applies to the processing of other data subject rights such as erasure requests, rectifications, objections and restrictions.

Microsoft SQL Server

Instead of an Access backend, a SQL Server database can also be used as the backend of an Access application. The Access frontend is largely retained in this constellation, but usually the data access must be adapted for performance reasons.

There are several reasons to migrate an Access database to a SQL Server database. In the context of data protection and data security, the reliability and access protection are of particular importance here. After all, these two belong to the security of the processing required by data protection, which - as already described above - is to be realized by technical and organisational measures. The following measures are listed in the GDPR:

- Ensuring the integrity and confidentiality of systems and services
- Pseudonymisation and encryption
- Ensuring system availability, resilience and recoverability
- Test, evaluate and assess the effectiveness of the measures taken

With integrity, confidentiality and availability, this enumeration contains the three classic goals of information security. On closer examination of the required measures, the GDPR does not call for anything new here. Pseudonymisation and encryption should be regarded as means of ensuring confidentiality and the resilience of systems and services is a component of their availability.

SQL Server offers multiple options for almost any of these goals. Some of them affect data access from Access to SQL Server. In such cases, changes in the Access application are required.

Integrity and confidentiality

Integrity refers, among other things, to the processing of correct data and tracking of data changes. The correctness of the data in SQL Server can be achieved by declarative integrity using foreign keys, unique keys etc. For the purpose of procedural integrity checking, SQL Server provides stored procedures, views, functions and triggers.

There are several ways to track data changes:

- Temporal Tables
  Automatically save older versions of records in a separate table
- Change Data Capture
  Collect the changed data of a record for further processing
- Change Tracking
  Collect information about what type of change has been made to a record
- OUTPUT
  Supplement for the commands INSERT, UPDATE and DELETE to output the added, changed or deleted values
- Triggers
  Custom programming in an After Trigger to log the changes

Confidentiality is the protection of information from unauthorised access. This protection can be achieved by means of classic authorisation assignments, as well as by pseudonymisation and encryption as required by the GDPR.

Access control

SQL Server provides a multi-level security architecture. It consists of access control at the SQL Server instance level and access control for each individual database.

Within the databases, rights can be assigned to database objects such as tables, views, stored procedures etc. via database roles and schemas. In addition, access control according to a custom, defined business logic is possible via "Row Level Security" and data masking via "Dynamic Data Masking".

Pseudonymisation

The pseudonymisation of data in SQL Server can only be realised by custom concepts and development of custom functions.

Encryption

SQL Server provides certificates, symmetric and asymmetric keys for encryption. These encryption methods can be combined and used at different levels.

With special T-SQL functions, data in individual columns can be encrypted during UPDATE and INSERT and decrypted again during SELECT. The functions used depend on the encryption method used. There are some for the use of symmetric keys, asymmetric keys and certificates.

The "Always Encrypted" feature introduced with SQL Server 2016 takes a different approach. The protection of the encrypted data is handled by certificates that are managed outside of SQL Server. Users with access to the corresponding certificate can read the plain text of the data, but users without a certificate cannot. In this way, it is possible, for example, to prevent a database administrator from reading or changing data without permission.

The encryption and decryption when reading and writing data is done automatically. However, there are some rules to be observed for this automatic data access. These are comprehensively described in the documentation of the respective SQL Server version, as well as the limitations in interaction with other functions of SQL Server.

With "Transparent Data Encryption" (TDE) it is also possible to encrypt the database files. Microsoft speaks here of "encrypting data at rest". This is very true, because the data is only encrypted in the database files. It is decrypted when it is loaded into the main memory and encrypted again when it is written to the files. This is done automatically using a certificate. The transfer of data from SQL Server to the client and vice versa remains unencrypted. TDE has been available in the Standard Edition since SQL Server 2019, but in previous versions it is only available in the Enterprise Edition.

In addition to the data and databases, it is also possible to encrypt the database backups. This is done on the basis of a certificate. Without this certificate, the backup cannot be read or restored. In this way, the backup files are well protected against misuse.

The transport encryption of the data between SQL Server and client is of particular importance if their communication takes place via public or not well secured networks. Neither the source code of the Access application nor the SQL Server database needs to be adapted for this. The encryption of the network communication is activated by a corresponding configuration in SQL Server and ideally supplemented with the options of the used driver. Then the encryption takes place when the connection is established via SSL/TLS.

Availability, resilience and recoverability

To ensure availability and resilience, in addition to high availability with AlwaysOn, SQL Server offers the option of database mirroring and transaction log shipping.

In addition to the current database, these functions provide a second version of the database on a separate SQL Server. If one SQL Server fails, the system switches to the second SQL Server. Depending on the configuration, this is done automatically or manually.

SQL Server provides built-in functionality for database backup. The full backup creates a complete backup of the database, while the differential backup saves the changes since the last full backup. A special feature is the transaction log backup. Well planned, it prevents major data loss in the event of a crash. The shorter the cycle of a transaction log backup, the less data loss.

The usability of data backups must be checked regularly. Successful data recovery is only possible with intact data backups.

Test, evaluate and assess effectiveness

The cost of this requirement should not be underestimated. It is therefore good that SQL Server can be used to automate such checks. There are a number of functions for this:

- Login Auditing
  Logging successful and unsuccessful logons
- SQL Server Level Auditing
  Logging changes to the configuration of a SQL Server instance
- Database Level Auditing
  Logging changes to the configuration of a database
- Vulnerability Assessment
  Analysis, evaluation and reporting of the security risks of a database
- Policy-Based Management
  Automated monitoring of configured properties
- Extended Events/XEvents
  User-defined logging of events

Classification and rights of data subjects

In addition to the security of the processing, SQL Server also offers support with the organisational requirements for data protection. In theory, personal data can be classified in databases using the "Classify Data" function. The use of Extended Properties as a storage location for the classification is a sensible approach. In practice, this type of classification is unfortunately not usable due to the lack of user-friendliness.

SQL Server Integration Services can be used to comply with the right to data portability of data subjects. Using specially created SSIS packages, a person's data is read from a wide variety of data sources, transformed into a uniform format and stored. If a data subject requests the right to data portability, only the SSIS package must be executed.

Similarly, the use of SQL Server Reporting Services is conceivable for fulfilling the obligation to provide information. Specially defined reports provide the information to answer a request.

Conclusion

Data protection is largely perceived as a nuisance - and yes, it means additional administrative burdens. On the other hand, the conscious and careful handling of information about people should be a matter of course. Reality often looked and still looks different:

For many years, new functions and better evaluation options were the almost exclusive requirements for software development. Due to lack of time and budget, secure processing and IT security in general were not integrated into the software and neglected in the organisational handling of the data. We see the consequence in the almost daily reports on data protection violations and security breaches.

The GDPR is directed against these grievances. It aims at more security in processing and with "data protection by design and by default" it calls upon us software developers to rethink. We are able to increase the processing security in our database applications. This not only makes the software qualitatively better and more professional, but increasingly represents a competitive advantage. The GDPR promotes public awareness and higher data protection budgets through its advertising effect and its threats of punishment.

In order to participate, you need expert knowledge about data protection, data security and especially the GDPR. By now this has to be part of the equipment of every database developer. This whitepaper provides a contribution to this.

Appendices

- Checklist Inventory
- Record of processing activities

Checklist Inventory

Company

- Company structure
  - Sole proprietorship, group, independent company, locations, branches
- Goal and purpose of the company
  - IT system house, trade with personal data, retail trade etc.
- Staff
  - In-house and field staff, part-time employees, interns, students
- Data protection
  - Appointed Data Protection Officer
- Clients
  - Categories of customers (industry, size)
  - Particularities with regard to personal data (sensitive data, mass data)
  - Domestic, EU, non-EU
- Suppliers
  - Categories of suppliers
  - Domestic, EU, non-EU
  - External service providers who provide services for the company e.g. tax consultants and payroll accountants, IT service providers, independent sales representatives, cleaning staff, disposers for waste as well as for the destruction of files and data carriers, marketing agencies, printers, lettershops

Premises

Inclusion of all points with regard to access by employees and external parties such as customers, suppliers, service providers

- Buildings
  - Access, doors, keys, biometric recognition etc.
- Registration procedure
  - Visitor directory on paper with signature, name badge
- Rooms
  - Office, workshops, archives
  - Elevator with card access
  - Filing cabinets, safes etc.

Example:
After all the places had been recorded, the secretary made another comment: "and the boss collects everything that interests him in an unlocked cupboard behind his desk, invoices, customer letters, employee evaluations..."

Equipment and machinery

- Video surveillance and photography
- Vehicles
  - Location data, time recording, logbook, navigation systems etc.
- IoT and sensors

- Voice control
    - Alexa, Cortana, Siri & Co.
      for company smartphones as well as private smartphones of the employees
- Shredders
- Medical devices with patient data

Hardware

- IT infrastructure
    - Network, servers, clients, switches, telephone systems etc.
    - Printers and scanners, in particular leasing devices
- Mobile devices
    - Notebooks, smartphones, tablets
    - Bring your own device (BYOD) → mix private/professional/external data and control
- External storage media
    - USB sticks, hard disks, backup tapes
- Other equipment with potential security vulnerabilities
    - Smart TV, whiteboards, surface hubs, IP cameras, sensors (IoT) etc.

Example:
Due to the heat in the summer of 2018, the air conditioning in the server room failed. The servers had to move into the basement in a rapid mission, because there was the coolest room.

At first glance, this may have nothing to do with data protection. However, the GDPR stipulates that availability and operational safety must be guaranteed. It is questionable whether the also required confidentiality was still given by access protection after the move to the basement.

Software

- Operating systems
    - Servers, clients, virtual machines
- Configuration software for devices like printers, scanners, cameras etc.
- Office software
    - Contents of files and documents
    - Document management software, Sharepoint
- Email software
    - Mail contents and attachments
    - Central mail server and/or client software with offline function
    - Mail apps on mobile devices
- Mobile device management
    - Central control of mobile devices, in particular the apps installed there
    - Apps with location determination, tracking functions etc.
- Commercial software
    - ERP, financial accounting, CRM, payroll accounting
- Technical software
    - CAD, machine controls etc. (because of employee data, logins, contact persons)
- Tools
    - PDF printers, ZIP programs and other tools with possible tracking functions
- Custom software

    - Database applications with Access and SQL Server
    - Excel buildings, Power Pivot, Power BI
- File repository
    - Transfer folders
    - Data exports, source and destination directories of data imports/exports

Example:
After the installation of a remote access for an external developer (one of the authors) came as last point from the corporate IT: "and now install the app on your smartphone, which will send you the currently valid password".

In principle, there are no objections to the sending of the password. Only here, the external was required to install a third-party app on his smartphone that he could not verify, which would no longer ensure the confidentiality and integrity of the data on his smartphone. The remote access was thankfully rejected despite losses of earnings.

Internet and services

- Company websites
    - Online shop, portal, forums, blog with comment functions
- Email provider and web hosting
- Used web applications
    - Google, webmail
    - Online banking, portals of service providers, newsletter senders, in particular websites with tracking tools
- Cloud services
    - Office 365, Azure, AWS, Google Docs
    - Dropbox, OneDrive etc.
- FTP server
- VPN accesses
- Communication
    - Telephone, mobile phone providers, DSL

Record of processing activities

Controller:
Andreas Maria Müller
Datengasse 42
17012 Dreiundzwanzig

Phone: 0123/123456-0
Eail: info@ammdb.de
Web: www.ammdb.de

Managing director/owner: Andreas Maria Müller

Data Protection Office: no DPO appointed

No	Processing activity	Contact person	Version	Purposes of processing	Lawful basis	Category of data subjects	Category of personal data	Special categories of data referred to in article 9	DPIA required	Profiling	Category of recipients	Third country transfer	Deletion periods	Storage locations	Technical organisational measures
1	**customer administration**	Emma Stein 0000/7890123 es@ammdb.de	processing activity introduced: 2018-03-02 last modified: 2019-03-03	contract fulfilment pre-contractual measures administration of master data	contract fulfilment pre-contractual measures	customers, contact person, employees, participating business partners	name, address, e-mail, telephone, tax number, bank details, contract texts and business correspondence customer contact history	none	no	no	banks, tax consultant, participating business partners, e-mail provider, postal and parcel services	data exchange via Dropbox to USA (Dropbox on the list of members of the Privacy Shield)	max. 10 years (legal retention period)	databases, e-mail program, document files, Dropbox, files, archives, CRM	see directory of TOMs and IT security concept
2	**advertising measures for customer acquisition and retention**	…	…	advertising measures for customer retention	legitimate interests by the controller	…	…	…	…	…	…	…	…	…	…
	…														

Hint:
In addition to the provisions of article 30 of the GDPR, we have included a number of columns with useful additional information.
- Version – to be able to track changes
- Storage locations – in which offices, store room or which programs, databases etc. the data are located
- Lawful basis – additional information required by the German Bundesdatenschutzgesetz (Federal Data Protection Act, abbr. BDSG)
- Profiling – additional information required by the BDSG
- DPIA required – documents that a risk assessment and, where appropriate, a data protection impact assessment has been carried out. Depending on the result, the column could contain a reference to the documentation of the risk assessment or the DPIA.