CyberWehr

RISK MANAGEMENT SOLUTIONS GMBH

Monika Wehr ▪ Alte Landstrasse 109 ▪ 8803 Rüschlikon ▪ Telefon +41 (0) 79 348 55 63

Directory of processing activities (DPA)

Pursuant to Art. 12 DPA and 30 GDPR, the creation of a register of processing activities is mandatory for most companies in order to demonstrate ("accountability") that the data protection requirements are met on an ongoing basis, also for a case in the past, in the company's practice.

The DPA is a central component of the documentation obligation vis-à-vis the supervisory authorities and can, for example, become the basis for risk assessments by the DPO for his and the DPO's own risk-oriented monitoring mandate (Art. 39 (2) GDPR). Without such structured documentation, the data protection officer's advisory and monitoring duties can hardly be implemented. Internal extensions of the DPA by risk assessments or an additional structuring are conceivable, which records which processing operations require a data protection impact assessment and which do not. In addition, the audits performed can be included. But: The DPA must not be overloaded!

The documentation of "guarantees" required in connection with the transfer of personal data to bodies in third countries is not necessary in regular processes. Corresponding guarantees are to be documented exclusively in the cases of Article 49 (1) and (2) of the GDPR. Documentation of further guarantees, such as an adequacy decision by the Commission or standard contractual clauses, may be useful in order to comply with the accountability and transparency obligations of data subjects. Data subjects.

As a rule, all data controllers in companies, public authorities, etc. must maintain a DPA. According to the DSG and Art. 30 para. 5 DSG/Art. 7 DSG, this obligation is limited to companies and public authorities.

- ✓ with a size of 250 employees or more; or
- ✓ with a particular risk in the processing; or
- ✓ with processing of sensitive data (Art. 9 and 10 GDPR); or
- ✓ processing that is not only occasional.

However, this exception does not apply. At the latest, if regular processing is used as a basis, all data controllers are affected, regardless of their number of employees.

The DPA may be kept in an electronic format. Because of the obligation to submit it to the supervisory authority in Article 30 (4) of the GDPR, it must be exportable in electronic or printed form.

It is advisable here to bundle processing operations according to a purpose. This processing directory contains a number of processing operations that occur in almost every company. These can be freely used as an aid to the creation of the directory. The information is to be adapted individually to the company in each case.

The contents of the DPA for data controllers derive from Art. 30 (1) GDPR and include:

- the name and contact details of
  - the person responsible (i.e., as a rule, naming of the company);

    - persons authorized to represent the company (in the case of a limited liability company, e.g., the managing directors)
    - if applicable, of the jointly responsible person;
    - If applicable, the representative in the EU;
    - if applicable, the data protection officer at the controller;
- the purposes of the processing;
- the categories of data subjects;
- the categories of personal data;
- the categories of recipients to whom personal data have been or will be disclosed;
- where applicable, transfers of personal data to a third country or to an international organization
    - including the indication of the third country or international organization concerned;
    - in the case of data transfers referred to in Article 49(1)(2) of the GDPR, the documentation of appropriate safeguards;
- [if possible,] the time limits foreseen for the deletion of the different data categories;
- It is expected that a general description of the technical and organizational measures according to DSG Art. 7 and Art. 32 para. 1 GDPR is available.

In addition, the legal basis for the processing must also be listed.

Examples of typical processing operations are:

- Collection
- website
- controlling
- applicant management
- CRM
- e-mail management
- Purchasing
- Facility Management
- Financial Accounting
- Freelancer database
- Fleet Management
- IT MANAGEMENT
- contact management
- payroll accounting
- marketing
- Personnel - HR
- Production Management
- Project Management
- Auditing - Compliance
- Appointment management
- Sales - Distribution
- Administration
- video surveillance
- Time Recording

Description of the purposes of processing

- **Collection:** assertion and enforcement of payment claims.
- **Website:** Operation of a website for the external presentation of the company and for contacting including contact form
- **Controlling:** Planning, management and control of all areas of the company

- **Applicant management:** The purpose of applicant management is recruitment. This includes finding suitable applicants and selecting the applicants with the best skills for the respective position.
- **Customer Relationship Management (CRM):** Maintaining customer relations and relationships with prospective customers.
- **E-mail:** Electronic communication
- **Purchasing:** purchasing of goods or services
- **Facility Management:** Care and maintenance of real estate and buildings used by the company.
- **Financial Accounting:** Determination and management of all income and expenses, especially for the purpose of determining and paying taxes and duties.
- **Freelancer database**: management of contacts and skills of freelancers.
- **Fleet management:** administration of vehicles used by the company
- **IT:** provision, maintenance and servicing of IT systems
- **Contact management:** management and provision of contacts of people, companies or public bodies
- **Payroll accounting:** Determination of wages & salaries, payroll accounting and payment of wages & salaries
- **Marketing:** marketing/advertising of goods or services and for the company as a whole.
- **Personnel - HR:** processing of personal data, personnel development
- **Production:** production of goods or services
- **Project management:** management of projects in the company Distribution: sale and distribution of goods or services.
- **Audit - Compliance:** Review of the legal conformity of business processes in the company.
- **Appointment management:** planning and management of appointments
- **Sales - Distribution:** Sale and distribution of goods or services
- **Administration:** General administration of the company (organization, office organization
- **Video surveillance:** exercising of domiciliary rights, assertion of claims, prosecution of criminal offenses
- **Time recording:** recording of working, attendance, absence and vacation times

Description of the categories of personal data

- **Collection of outstanding debts:** first name, last name, company name, address (business), address (private), billing address, Internet address, e-mail address, telephone number, fax number, position, industry, customer number, type of customer, contact data, contact history, bank details, wage garnishment data, solvency data, non-payment risk data, scoring data.

- **Website:** Name, company name, inventory data, usage data, content data

- **Controlling:** first name, last name, company name, address (business), billing address, e-mail address, telephone number, fax number, position, industry, customer number, customer type, contact data, contact history, contract data, inventory data, usage data, sales data

- **Applicant management:** first name, last name, title, curriculum vitae, school-leaving qualification, professional qualification, studies

- **Customer Relationship Management (CRM**): first name, last name, title, company name, address (business), Internet address, e-mail address, telephone number, fax number, marital status, customer number, customer type, contact data, contact history, appointment data, data on interests, goods purchased, communication data, photos, information on profession

- **E-mail:** Name, e-mail address, usage data, traffic data

- **Purchasing:** first name, last name, company name, address (business), billing address, e-mail address, phone number, fax number, position, contact history, bank details, VAT ID number, data on purchased goods or services, contract data, sales data

- **Facility Management:** first name, last name, company name, address (business), email address, phone number, fax number, contact data, contact history, appointment data, contract data, photos
- **Financial accounting:** Determination and management of all revenues and expenditures, in particular for the purposes of determining and levying taxes and duties
- **Freelancer database:** First name, last name, title, company name, address (business), billing address, Internet address, e-mail address, telephone number, fax number, position, contact data, contact history, appointment data, contract data, communication data, fo-tos, professional and career data, school-leaving certificate, professional degree, studies, training data
- **Fleet management:** First name, last name, address (business), address (private), e-mail address, telephone number, date of birth, position, driver's license data
- **IT:** First name, last name, title, email address, phone number, position, contact history, usage data, traffic data, telecommunication data, communication data.
- **Contact management:** first name, last name, address (business), address (private), billing address, Internet address, e-mail address, telephone number, fax number, position, industry, customer number, customer type, contact data, contact history, appointment data.
- **Payroll:** first name, last name, title, address (private), telephone number, date of birth, marital status, details of dependents (children), bank details, contract data, social security data, working hours, wage and salary data, details of tax classes, religious affiliation, details of wage garnishments
- **Marketing**: first name, last name, title, company name, address (business), Internet address, e-mail address, telephone number, fax number, position, industry, customer number, customer type, contact history, appointment data, data on interests
- **Personal – HR**: first name, last name, title, address (private), telephone number, e-mail address, date of birth, marital status, data on dependents (children), health data, data on interests, bank details, contract data, photos, social security data, working hours, wage and salary data, data on tax classes, religious affiliation; data on occupation, career and wage garnishments, vacation periods, data on occupational integration management, school and vocational qualifications, studies, sick days, data on previous convictions or entries in the Federal Central Register, data on further vocational training.
- **Production**: name, company name, address (business), address (private), billing address, e-mail address, telephone number, fax number, position, industry, customer number, customer type, working hours, sales data
- **Project management:** first name, last name, company name, address (business), e-mail address, telephone number, fax number, position, industry, appointment data, contract data, communication data, sales data
- **Revision – Compliance**: First name, last name, e-mail address, telephone number, date of birth, marital status, position, contact data, contact history, appointment data, bank connection, VAT ID number, data on purchased goods or services, contract data, sales data, usage data, content data, communication data, social insurance data, working hours, wage and salary classes, information on tax classes, religious affiliation; information on profession, professional career, data on criminal records or entries in the Federal Central Register, data on professional training.
- **Appointment management:** first name, last name, company name, address (business), address (private), e-mail address, phone number, position, contact data, appointment data

- **Sales - Distribution: :** First name, last name, title, company name, address (business), address (private), e-mail address, phone number, customer number, customer type, contact data, contact history, appointment data, bank details, VAT ID number, data on purchased goods or services, contract data, turnover data**.**

- **Administration:** first name, last name, title, company name, address (business), e-mail address, phone number, position, contact data, contact history, contract data

- **Video surveillance:** name, videos, description of categories of data subjects, employees, customers, prospects, service providers, visitors

- **Time recording:** first name, last name, e-mail address, working hours, vacation time, sick days, description of categories of data subjects, employees, temporary workers

Description of the categories of persons concerned

- **Debt collection:** customers, third parties
- **Website:** interested parties, visitors
- **Controlling:** employees, customers, service providers, third parties
- **Application management:** applicants
- **Customer Relationship Management** (**CRM):** employees, customers, prospects
- **E-Mail:** employees, Customers, interested parties, service providers, third parties
- **Purchasing:** employees, service providers, third parties**,** creditors
- **Facility Management**: employees, service providers, third parties
- **Financial accounting:** employees, customers, debtors, creditors
- **Freelancer-database:** service providers, third parties
- **Fleet management:** employees
- **IT:** employees, customers, service providers, third parties
- **Contact management**: employees, customers, interested parties, third parties
- **Payroll accounting**: employees
- **Marketing**: employees, customers, interested parties, third parties – purchased goods data: contract data, photos, videos
- **Personnel – HR**: employees
- **Production**: employees, customers, interested parties, service providers, third parties
- **Project management**: employees, customers, service providers, third parties
- **Audit – Compliance**: employees, customers, service providers, third parties
- **Contact Management**: employees, customers, interested parties, service providers, third parties
- **Sales – distribution**: customers
- **Administration**: employees, customers, interested parties, service providers, third parties
- **Video surveillance**: employees, customers, interested parties, service providers, third parties
- **Time recording**: first name, last name, e-mail address, working hours, vacation time, sick days, description of categories of data subjects, employees, temporary workers

Categories of recipients to whom the personal data have been or will be disclosed

- **Debt collection:** lawyers, credit agencies, law enforcement agencies
- **Website**: plus Hosting-Provider, possibly or internal departments for processing enquiries
- **Controlling:** interested parties
- **Applicant management:** works council, internal offices responsible for hiring the applicant
- **Customer Relationship Management (CRM)**: CRM service providers, employees in the company, processors
- **E-Mail:** service providers, other persons within the company, third parties if applicable
- **Purchasing:** internal departments that use goods or services, works council, third parties if necessary

- **Controlling**: Auditor, tax consultant, works council, company management
- **Facility Management**: Service providers who take over facility management services, other third parties if applicable.
- **Financial accounting:** tax office, auditor, tax consultant
- **Freelancer-Database:** internal departments that have freelancer needs, works council
- **Fleet management:** Owner of the vehicle (lessor), parties involved in the accident, motor vehicle liability insurer, third parties if applicable.
- **IT:** employees with personnel responsibility, works council
- **Contact Management**: internal departments or persons in departments
- **Payroll accounting:** works council, auditors, tax consultants, social security offices, health insurance companies, financial administration, insurers for company pension schemes, department heads or persons with personnel responsibility, company management.
- **Marketing**: Service providers used for marketing/advertising
- **Personnel – HR**: Works council, social security offices, health insurance funds, financial administration, insurers for company pension plans, department heads or persons with personnel responsibility, company management
- **Production**: Cooperation partners, suppliers, customers, sales and trading partners
- **Project Management:** works council
- **Audit – Compliance**: Auditor, tax consultant, works council, company management
- **Appointment management:** other participants in appointments
- **Sales – Distribution**: Cooperation partner, logistics company
- **Administration:** internal departments, service providers, third parties if necessary
- **Video surveillance**: Lawyers, law enforcement agencies
- **Time recording** works council, auditor, tax consultant

If applicable, transfer of personal data to a third country or to an international organization

- **Website**: integration of Google Web Fonts. In this context, Google servers in the USA are called up. Google is the "controller" for the processing. The adequate level of data protection results from Google's participation in the Privacy Shield.
- **Controlling:** none
- **Applicant management**: not planned
- **Customer Relationship Management (CRM):** A software system of a service provider in a third country (here: USA) is used for the CRM system. There is an order processing agreement with the service provider. The appropriate level of data protection is guaranteed by the service provider's membership in the "Privacy Shield".
- **E-Mail:** Not planned. Nevertheless, when e-mails are sent via the Internet, it can never be ruled out that they are forwarded via a third country.
- **Purchase:** none
- **Facility Management:** none
- **Financial accounting**: none
- **Freelancer-Database :** none
- **Fleet Management:** none
- **IT:** none
- **Contact Management:** none
- **Payroll Accounting**: none
- **Marketing**: none
- **Personal – HR**: none
- **Production**: none
- **Project administration**: none
- **Revision – Compliance**: none
- **Sales - Distribution**: none
- **Administration**: none
- **Video surveillance**: none

- **Time recording** none

Provided deadlines for the deletion of the different categories of data

Debt collection: Data on the assertion of outstanding claims is stored for at least 10 years. After 10 years, a check is made at the end of the calendar year to determine whether the claim is still enforceable (enforcement title). If an enforcement order exists, the data will be stored until the enforcement order becomes time-barred, unless the claim has been settled by the debtor or a third party beforehand.

Website: Usage data is deleted or anonymized after 7 days at the latest. Content data (e.g. data submitted via a contact form) is stored for a period of 1 year. After the end of the year, a further requirement for storage is checked and a new check is scheduled at the end of each calendar year. If content data is to be classified as a business letter, the retention obligations under commercial law apply.

Controlling: Data processed for controlling purposes is generally stored for a period of 10 years. After this period has expired, a check is made at the end of the respective calendar year to determine whether further storage is necessary. If this is not necessary, the data is deleted.

Applicant management: Applicant data is generally deleted 6 months after the respective position has been awarded. An exception to this is the data of applicants who have given their consent to the continued storage of their data in the applicant data pool. In the case of this data, a check is carried out after two years to determine whether there is a need for further storage. Otherwise, the data will be deleted.

Customer Relationship Management (CRM): In the case of personal data in the CRM system, a check is made after two years at the end of the respective calendar year to determine whether further storage is necessary. If it is not necessary, the data is deleted. An exception to this is data that is to be classified as business letters within the meaning of the German Commercial Code (HGB) or as accounting-relevant data. Here, the respective statutory retention obligations apply.

E-Mails are stored for at least 6 years in order to comply with the retention requirements for business letters under commercial law. After 6 years, a check is made at the end of the respective calendar year to determine whether further storage is necessary. If this is not necessary, the data will be deleted. An exception to this is data that is to be classified as accounting-relevant data. In this case, the respective retention obligations under tax law apply.

Purchase: For data from purchasing, the retention obligations of 6 years under commercial law are observed. After 6 years, the data will be checked. If there is no need for further storage, the data will be deleted.

Facility Management: Data on maintenance and servicing work carried out is stored for a period of 4 years. After four years, a check is made at the end of the respective calendar year to determine whether further storage is necessary. If there is no need, the data will be deleted.

Financial accounting: Financial accounting data is stored for at least 10 years in accordance with the requirements of the German Fiscal Code (AO). Section 147 (4) AO applies to the start of the period.

Freelancer Data is stored for a period of 4 years. After four years, a check is made at the end of the respective calendar year to determine whether further storage is necessary. If there is no need, the data will be deleted.

Fleet management: Data of employees who use or can use vehicles from the fleet are stored for the duration of the employment relationship. The data of data subjects are generally deleted 4 years after the end of an employment relationship at the end of a calendar year.

IT: There are many different storage periods for personal data processed in the IT sector. These depend on the respective application or IT system and differ.
In IT systems with which personal data is processed, there is usually a logging function with which it can

be traced "who" has "entered, changed or deleted" "which data" at "which time". This log is usually stored for a further 4 years from the deletion of the respective data record. At the end of each calendar year, a check is made to determine whether data can be deleted.
In addition, for generally occurring data in the area of IT (processing of orders, requirements, etc.), it applies that for this data, it is checked after four years at the end of the respective calendar year whether further storage is necessary. If this is not necessary, the data will be deleted.
An exception to this is data that is to be classified as business letters within the meaning of the German Commercial Code (HGB) or as accounting-relevant data. Here, the respective statutory retention obligations apply.

Contact Management: In the case of personal data, a check is made after four years at the end of the respective calendar year to determine whether further storage is necessary. If there is no need, the data will be deleted.

Payroll accounting: Two years for the recording of overtime.
Tax-relevant data is stored for at least 10 years in accordance with the requirements of the German Fiscal Code. Section 147 (4) AO applies to the start of the period.
All other data is stored for a period of two years; at the end of the calendar year, it is checked whether further storage is required. If there is a requirement, the necessity will be reviewed again annually at the end of each calendar year.

Marketing: In the case of personal data processed for advertising purposes, checks are generally carried out at the end of a calendar year to determine whether there is a need for further processing of the data. Depending on the result, data will be further stored or deleted.

Personnel – HR: Warnings: 36 months.
Otherwise, after 10 years after termination of the employment relationship, it will be checked whether deletion can take place. Deletion will not take place if the employee wishes to take or is taking a company pension.

Production: Data arising in connection with production are stored for a period of 6 years. The basis for the storage period is that data from production may be related to warranty and guarantee claims and may be required for the defense against claims or for the examination of claims.
In addition, data from production as a business letter may be subject to the retention obligations under the German Commercial Code (HGB).
The storage of data is reviewed and adjusted at least annually with regard to data classifications.

Project Management: In the case of personal data in project management, a check is made after four years at the end of the respective calendar year to determine whether further storage is necessary. If this is not necessary, the data is deleted.
An exception to this is data that is to be classified as business letters within the meaning of the German Commercial Code (HGB) or as accounting-relevant data. Here, the respective statutory retention obligations apply.

Audit – Compliance: Data processed for auditing or compliance purposes is generally stored for a period of 10 years.
After this period has expired, a check is made at the end of the respective calendar year to determine whether further storage is necessary. If there is no need, the data will be deleted.

Appointment management: In the case of personal data in appointment management, a check is made after four years at the end of the respective calendar year to determine whether further storage is necessary. If this is not necessary, the data will be deleted.
An exception to this is data that is to be classified as business letters within the meaning of the German Commercial Code (HGB) or as accounting-relevant data. Here, the statutory retention obligations are taken into account.

Sales - Distribution: In the case of personal data relating to sales/distribution, it must be assumed that this data is relevant to accounting. Therefore, the data is generally stored for 10 years, whereby the start of the period is determined by Section 147 (4) of the German Fiscal Code (AO).

Administration: In the case of personal data relating to general administration, a check is made after four years at the end of the respective calendar year to determine whether further storage is necessary. If there is no need, the data will be deleted.
An exception to this is data that is to be classified as business letters within the meaning of the German Commercial Code (HGB) or as accounting-relevant data. Here, the respective statutory retention obligations apply.

Video surveillance: Video recordings are deleted after 10 days at the latest.

Time recording - Provided deadlines for the deletion of the different categories of data: Overtime: 2 years. Tax-relevant data of the working time recording are stored for at least 10 years according to the requirements of the tax code. All other data is stored for a period of two years. At the end of the calendar year, it is checked whether further storage is necessary. If this is not the case, the data will be deleted.

The relevant legal bases in each case - Notes on the prioritization of the compliance checks of the data processing operations:

B2B companies: the most sensitive data processing is usually the company's own employees, in B2C companies the data of consumers (customers) and the core activities of the company. Less sensitive are data from suppliers and corporate customers (even if they contain employee data), data from public sources and data whose processing is strictly regulated by law or by third parties anyway.

The following criteria can help to identify particularly sensitive data processing. If two of them are given, this is even an indication of high risk under the GDPR, which again requires a data protection impact assessment:

1. Data is analyzed in depth, scoring or other forms of profiling take place.
2. Automated individual decisions are made on the basis of the data, which have a legal effect on the data subject or significantly affect him or her in a similar way.
3. Systematic monitoring takes place, or it is not possible for the persons concerned to evade the collection of data.
4. Special categories of personal data (→ Glossary) of data on criminal convictions and criminal offenses are processed.
5. Data is processed in a comprehensive manner, whether in terms of the number of persons concerned, the volume and variety of data, the duration or permanence of the data processing, or the local spread of the data processing.
6. Different data collections and sources are combined or compared with each other.
7. To process the data of particularly vulnerable persons, such as children, employees, persons with mental disorders, asylum seekers, patients, the elderly or other persons in a dependent relationship.
8. Data processing is based on innovative technology or other new forms of organization, the negative consequences or risks of which are not yet fully known.
9. The data processing serves to determine to whom a service or a contract should be offered, or otherwise complicates the exercise of rights by the persons concerned.
10. If a data processing operation could be considered sensitive by the public or could have lasting and significant negative consequences for a data subject, whether carried out correctly or improperly, this data processing operation should be assessed as a priority.

Examples of data processing for a medium-sized company (B2C):

Human resources - Personnel administration
Human resources - payroll accounting
Human resources – Recruitment
Human Resources - Health and Safety
Human Resources - Training Management
Human Resources - Career Development
Marketing & Sales - Customer Data Management

Marketing & Sales - Customer Accounting, Billing & Payments Marketing & Sales - Customer Loyalty Program

Marketing & Sales - Marketing, Customer Events Marketing & Sales - Customer Service

Marketing & Sales - Online Shop
Marketing & Sales - App

Marketing & Sales – Newsletter
Marketing & Sales - Market Research
Marketing & Sales - Product development and testing Suppliers & Partners - Supplier management Suppliers & Partners - Online procurement platform Suppliers & Partners - Dealer management, suppliers & partners – Promoters
Suppliers & Partners - Contract Management

Financial management - Finance and accounting
Financial management - Expense management
Financial management - Real estate, financial assets Communication - Internal communication
Communication - Media office

Communication – Website
Logistics & Operations - Video Surveillance
Logistics & Operations - Building Access Control
Logistics & Operations - Visitor Data Management
Logistics & Operations - Fleet Management
Logistics & Operations - Facility Management
Information technology - Directory services
Information Technology - E-mail System
Information Technology - Document Storage
Information Technology - Network Monitoring
Information Technology - Device Management
Company – Legal
Company - Shareholder administration
Company - Administration Board of Directors and Management Company - Internal Audit
Company - Internal investigations