**Review schedule: Requirement to conduct a data protection impact assessment in accordance with Article 35 of the General Data Protection Regulation for the private sector**

**A data protection impact assessment (DPIA) is a structured risk assessment for the prior evaluation of the possible consequences of data processing operations. A DPIA should be carried out where there is likely to be a high risk to the rights and freedoms of natural persons by virtue of the nature, scope, context and purposes of the processing.**

**You can use this review schedule to check whether a DPIA is required for your area of responsibility. Data protection officers (internal or external) can and should be involved in this process and be asked for advice. Transmission to the State Commissioner for Data Protection of Lower Saxony is not required*.***

If you conclude that you do need to carry out a DPIA, you should first prepare a systematic description of the intended processing activities and the purposes of the processing. On this basis, you must then carry out an appropriate risk analysis for the processing. The law does not prescribe how a data controller should approach this task. However, in order to fulfill the purpose of a DPIA – to plan actions which demonstrate compliance with the GDPR – it must be ensured that the outcomes of the methodology are transparent. To make this easier for you, LfD Lower Saxony (State Commissioner for Data Protection of Lower Saxony) has developed ZAWAS, a practical process to facilitate the selection of appropriate protective measures and simplify the associated risk analysis. You can find out more about this [here](https://lfd.niedersachsen.de/startseite/themen/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/zawas/praxisnahe-hilfe-zum-technisch-organisatorischen-datenschutz-173395.html).

*We have included a glossary at the end of this document. The various terms and phrases explained there are indicated in the text with italics.*

Contents

[Key details for the review and for the processing activity 3](#_Toc64647606)

[Review process at a glance 5](#_Toc64647607)

[A. Review of the list for the private sphere pursuant to Article 35(4) of the GDPR 6](#_Toc64647608)

[B. Review of Article 35(3) of the GDPR 15](#_Toc64647609)

[C. Review of Article 35(1) of the GDPR following Working Paper 248 (WP 248) 17](#_Toc64647610)

[D. Conclusion of the review 23](#_Toc64647611)

[Help on DPIAs 24](#_Toc64647612)

[Checklist 25](#_Toc64647613)

[Glossary 27](#_Toc64647614)

# Key details for the review and the processing activity

* Name and job title of the data controller:
* Intended processing activity:
* Description of the intended processing activity (*nature*, *scope*, *circumstances* and *purposes of the processing*)[[1]](#footnote-1):
* In addition to the description of the processing activity above, the following documents form the basis of the review:
* Where applicable, reference (number/letter) of entry in the *record of processing activities*:
* Date of review:
* Review carried out by (name(s) and job title(s)):

# Review process at a glance

Review of the list for the private sphere pursuant to Art. 35(4) of the GDPR: Is this kind of processing included on the “DPIA required” list of the
supervisory authorities?

Yes

No

Review of Article 35(3) of the GDPR:
Does the processing meet one of the criteria set out in Article 35(3) of the GDPR?

Conduct DPIA

Yes

No

Review of Article 35(1) of the GDPR in accordance with Working Paper 248:
How many of the criteria from WP 248 does the processing meet?

Conduct DPIA

Depending on the result, conduct DPIA or end review

# A. Review of the list for the private sphere pursuant to Article 35(4) of the GDPR

Pursuant to Article 35(4) of the GDPR, the supervisory authorities are obliged to draw up a “required list” of processing activities for which a DPIA must always be carried out. The list, which contains typical fields of application and examples to support the review, can be found [here](https://lfd.niedersachsen.de/startseite/datenschutzreform/ds_gvo/liste_von_verarbeitungsvorgangen_nach_art_35_abs_4_ds_gvo/muss-listen-zur-datenschutz-folgenabschatzung-179663.html).

A.1 Processing of biometric data for the purpose of uniquely identifying natural persons, where **at least one other of the following criteria** from [Working Paper 248 rev.01](https://lfd.niedersachsen.de/download/124733) of the Article 29 Working Party applies:

* data on *vulnerable data subjects,*
* *systematic monitoring,*
* *innovative use* or *application* *of new technological* or organizational solutions,
* evaluation or ranking (*scoring*),
* *matching* or *combining* datasets,
* *automated decision-making* with legal or similar significant effect,
* data subjects are prevented from the exercise of a right or use of a service or performance of a contract.

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable[[2]](#footnote-2):**

A. 2 Processing of *genetic data* within the meaning of Article 4(13) of the GDPR, if **at least one other of the following criteria** from [WP 248 rev.01](https://lfd.niedersachsen.de/download/124733) applies:

* data on vulnerable data subjects,
* systematic monitoring,
* innovative use or application of new technological or organizational solutions,
* evaluation or ranking (scoring),
* matching or combining datasets,
* automated decision-making with legal or other similar significant effect,
* data subjects are prevented from the exercise of a right or use of a service or performance of a contract.

[ ]  **Yes**

**☐ No**

**Reasons, if applicable:**

A.3 Processing on a large scale of data that are subject to social, professional or special official secrecy requirements, even if these are not data pursuant to Art. 9(1) and 10 of the GDPR.

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

A. 4 Processing on a large scale of personal data relating to the location of natural persons.

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

A.5 Combination of personal data from different sources and processing of the data so combined, provided that the combination or processing:

* is carried out on a large scale,
* is done for purposes for which not all of the data to be processed have been collected directly from the data subjects,
* involves the use of algorithms which are not transparent to the data subjects, and
* serves to generate data bases, which can be used to make decisions developing legal effects concerning the data subjects or which may affect them in a similarly significant way.

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

A.6 *Mobile optical-electronic collection* of personal data in public areas, where the data from one or more collection system(s) are combined centrally on a large scale.

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

A.7 Collection and publication or transfer on a large scale of personal data, which are used to evaluate the behavior and other personal aspects of individuals and which may be used by third parties to make decisions developing legal effects in relation to the persons evaluated or which affect them in a similarly significant way.

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

A.8 Processing of personal data on a large scale concerning the behavior of *employees,* which may be used to evaluate their work in such a manner resulting in legal consequences for the data subjects or otherwise affecting them significantly.

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

A.9 Profiling of the interests, network of personal relationships or personality of the data subjects on a large scale.

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

A.10 Combination of personal data from different sources and processing of the data so combined, where the combination or processing

* is carried out on a large scale,
* is done for purposes for which not all of the data to be processed have been collected directly from the data subjects,
* involves the use of algorithms which are not transparent to the data subjects, and
* serves for the discovery of previously unknown relationships between data for purposes not determined in advance.

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

A.11 Use of *artificial intelligence* to process personal data for the purpose of managing the interaction with data subjects or evaluating personal aspects of the data subject.

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

A.12 Unconventional use of sensors of a mobile device in the possession of the data subject or of *radio signals* transmitted by such devices to determine the location or movement of persons over a substantial period of time.

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

A.13 Automated analysis of video or audio recordings to assess the personality of the data subjects.

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

A.14 Profiling of the movement and purchasing behavior of data subjects on a large scale.

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

A.15 *Anonymization* of special personal data pursuant to Article 9 of the GDPR which is not merely carried out individually (in terms of the number of data subjects and the information per data subject) for the purpose of transfer to third parties.

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

A.16 Processing of personal data pursuant to Art. 9(1) and Art. 10 of the GDPR – even if it is not considered to be "on a large scale" within the meaning of Art. 35(3)(b) – provided that data collection takes place not merely a single time by means of the innovative use of sensors or mobile applications and that these data are received and processed by a central body.

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

A.17 Processing of data pursuant to Art. 9(1) and Art. 10 of the GDPR – even if it is not considered to be "on a large scale" within the meaning of Art. 35(3)(b) – provided that the data are used by providers of new technologies to determine the capacity of the individuals.

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

**Provisional conclusion:**

[ ]  **The answer “Yes” was given at least once.**

**A data protection impact assessment must be performed before the start of the processing activity. 🡪 Continue with step D.**

[ ]  **All questions were answered with "No".**

**Please continue with the review of whether you need to perform a DPIA pursuant to Art. 35(3) of the GDPR (next page).**

# B. Review of Article 35(3) of the GDPR

B.1 The activity involves systematic and extensive evaluation of personal aspects relating to natural persons based on automated processing including *profiling*,which, in turn, serves as the basis for decisions that develop legal effects in relation to natural persons or have similarly significant effect on them.

[ ]  **Yes**

[ ]  **No**

 **Reasons, if applicable:**

B.2 The activity involves large-scale processing of special categories of personal data pursuant to Article 9(1) of the GDPR or of personal data relating to criminal convictions and offenses pursuant to Article 10 of the GDPR.

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

B.3 The activity involves systematic and monitoring *of publicly accessible areas* on a large scale.

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

**Provisional conclusion:**

[ ]  **The answer “Yes” was given at least once.**

The processing meets the requirements of Article 35(3) of the GDPR.

**A data protection impact assessment must be performed before the start of the processing activity. 🡪 Continue with step D.**

[ ]  **All questions were answered with "no".**

The processing does not meet the requirements of Article 35(3) of the GDPR.

**Please continue with the review of whether you need to perform a DPIA pursuant to Art. 35(1) of the GDPR (next page).**

# C. Review of Article 35(1) of the GDPR following Working Paper 248 ([WP 248](https://lfd.niedersachsen.de/download/124733))[[3]](#footnote-3): a DPIA is only required if the processing is "likely to result in a high risk to the rights and freedoms of natural persons”.

C.1 Data subjects are evaluated or classified (profiling or forecasting the individual's job performance, economic situation, health, personal preferences or interests, reliability, etc.)

 [ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

C.2 The activity involves automated decision-making with legal effect or with a similarly significant effect (for example, data scoring in online retail or the insurance or credit industry; automated decision-making in job classifieds; automated decision-making for the income tax assessment).

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

C.3 The activity involves systematic monitoring (processing operations intended to observe, monitor or supervise data subjects, using, for example, data collected through networks).

 [ ]  **Yes**

[ ]  **No**

 **Reasons, if applicable:**

C.4 Sensitive or highly personal data are being processed.

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

C.5 The data processing is performed on a large scale.

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

C.6 Datasets are matched or combined.

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

C.7 Data on vulnerable data subjects, such as children, workers, the mentally ill, asylum seekers, the elderly or patients.

[ ]  **Yes**

[ ]  **No**

 **Reasons, if applicable:**

C.8 The activity involves innovative use or application of new technological or organizational solutions.

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

C.9 The processing may prevent data subjects from exercising a right or using a service or a contract.

[ ]  **Yes**

[ ]  **No**

**Reasons, if applicable:**

**Provisional conclusion:**

Click here to enter text of nine criteria have been met.[[4]](#footnote-4)

**Based on the criteria met, it is likely that a high risk to the rights and freedoms of data subjects:**

[ ]  **is present.**

**A data protection impact assessment must be performed before the start of the processing activity.**

[ ]  **is not present.**

**No data protection impact assessment is to be performed.**

Reasons/explanation, if applicable:[[5]](#footnote-5)

**Can a DPIA be omitted, in spite of the review result above?[[6]](#footnote-6)**

[ ]  **Yes**, because a DPIA has already been carried out for a similar processing operation with similar high risks (Art. 35(1) GDPR) and the measures set out there also apply to the present processing activity.

Name and internal reference of the DPIA in question:

Click here to enter text.

[ ]  **Yes**,because the processing activity started before 25 May 2018, a preliminary check was done by the Data Protection Officer or the supervisory authority and the risks to the rights and freedoms of data subjects have not changed.[[7]](#footnote-7)

Internal reference in the controller’s documentation for the preliminary check:

Click here to enter text.

A review will be carried out by Click here to enter text. as to whether there has been any change in the risks to the rights and freedoms of natural persons.

In the event of significant changes to the processing activity, the DPIA must also be updated or repeated.

[ ]  **No**

# D. Conclusion of the review

Before the processing activity is commenced:

[ ]  a data protection impact assessment must be carried out.

[ ]  no data protection impact assessment needs to be carried out.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of lead reviewer

**Review by data protection officer(s):**

The above review was audited on Click here to enter text.. The conclusion of the review above

[ ]  is endorsed.

[ ]  is not endorsed. Reason: Click here to enter text.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of the Data Protection Officer

**Concluding remarks:**

* For the purposes of accountability, you should complete and sign this review schedule and file it with the relevant data processing operation in your record of processing activities.
* If you have come to the conclusion that you must carry out a DPIA, you are required to appoint a data protection officer (§ 38 para. 1 sentence 2 of the German Federal Data Protection Act, BDSG).

# Help on DPIAs

* [Lists of processing operations requiring a data protection impact assessment according to Art. 35(4) GDPR](https://lfd.niedersachsen.de/startseite/datenschutzreform/ds_gvo/liste_von_verarbeitungsvorgangen_nach_art_35_abs_4_ds_gvo/muss-listen-zur-datenschutz-folgenabschatzung-179663.html)
* [WP 248, Guidelines on Data Protection Impact Assessment](https://lfd.niedersachsen.de/download/124733)
* [DSK Short Paper No. 5, Data Protection Impact Assessment](https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf)
* [ZAWAS process for selecting appropriate safeguards](https://lfd.niedersachsen.de/startseite/themen/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/zawas/praxisnahe-hilfe-zum-technisch-organisatorischen-datenschutz-173395.html)
* [Bavaria LDA on DPIA](https://www.lda.bayern.de/de/thema_dsfa.html)
* [Standard Data Protection Model](https://lfd.niedersachsen.de/startseite/themen/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/standard_datenschutzmodell/standard-datenschutzmodell-139069.html)

# Checklist

|  |  |  |
| --- | --- | --- |
| A. Review of the list pursuant to Article 35(4) of the GDPR  | Yes | No |
| A.1 | Biometric data for unique identification | [ ]  | [ ]  |
| A.2 | Genetic data within the meaning of Article 4(13) GDPR | [ ]  | [ ]  |
| A.3 | Social, professional or special official secrecy | [ ]  | [ ]  |
| A.4 | Data on the abode of natural persons | [ ]  | [ ]  |
| A.5 | Combination from different sources | [ ]  | [ ]  |
| A.6 | Mobile optical-electronic detection in public areas | [ ]  | [ ]  |
| A.7 | Evaluation of behavior and other personal aspects | [ ]  | [ ]  |
| A.8 | Conduct of employees | [ ]  | [ ]  |
| A.9 | Profiles of interests, relationships or personality | [ ]  | [ ]  |
| A.10 | Combination from different sources | [ ]  | [ ]  |
| A.11 | Artificial intelligence to manage interaction or to evaluate personal aspects | [ ]  | [ ]  |
| A.12 | Unconventional use of sensors of a mobile radio device or of radio signals | [ ]  | [ ]  |
| A.13 | Automated evaluation of video or audio recordings to assess personality | [ ]  | [ ]  |
| A.14 | Large-scale profiling of movement and purchasing behavior | [ ]  | [ ]  |
| A.15 | Anonymization of special personal data for the purpose of transfer to third parties | [ ]  | [ ]  |
| A.16 | Processing of data pursuant to Art. 9(1) and Art. 10 of the GDPR by means of the innovative use of sensors or mobile applications | [ ]  | [ ]  |
| A.17 | Processing of data pursuant to Art. 9(1) and Art. 10 of the GDPR in order to determine the capacity of individuals | [ ]  | [ ]  |

|  |  |  |
| --- | --- | --- |
| B. Review of Article 35(3) of the GDPR | Yes | No |
| B.1 | Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling | [ ]  | [ ]  |
| B.2 | Large-scale processing of special categories of data pursuant to Article 9(1) of the GDPR or of data relating to criminal convictions and offenses pursuant to Article 10 of the GDPR | [ ]  | [ ]  |
| B.3 | Systematic monitoring of publicly accessible areas on a large scale | [ ]  | [ ]  |

|  |  |  |
| --- | --- | --- |
| C. Review of Article 35(1) of the GDPR following Working Paper 248 | Yes | No |
| C.1 | Data subjects are evaluated or classified (profiling or forecasting) | [ ]  | [ ]  |
| C.2 | Automated decision-making with legal effect or similarly significant effect | [ ]  | [ ]  |
| C.3 | Systematic monitoring | [ ]  | [ ]  |
| C.4 | Sensitive or highly personal data are processed. | [ ]  | [ ]  |
| C.5 | Large-scale data processing | [ ]  | [ ]  |
| C.6 | Datasets are matched or combined | [ ]  | [ ]  |
| C.7 | Data on vulnerable data subjects | [ ]  | [ ]  |
| C.8 | Innovative use or application of new technological or organizational solutions | [ ]  | [ ]  |
| C.9 | The processing may prevent the data subjects from the exercise of a right or use of a service or performance of a contract. | [ ]  | [ ]  |

# Glossary

|  |  |
| --- | --- |
| Anonymization | Anonymization is the modification of personal data with the result that the personal reference is irreversibly removed. In addition to the removal of identifying characteristics, anonymization can be achieved by aggregating personal data records, i.e. combining and abstracting data records each containing a personal reference to a person.  |
| Matching of datasets | Dataset matching is the process of examining records that originate from different data processing operations, which have been performed for different purposes, to see if they match.  |
| Type of processing | The type of data processing covers all the essential characteristics that distinguish the processing operation. The following factors should be considered in determining the type of processing: * Characterization of the processing operation: Art. 4([2)](https://beck-online.beck.de/?typ=reference&y=100&a=4&g=EWG_DSGVO&n=2) GDPR specifically mentions collection, recording, transmission, structuring, storage, erasure and destruction.
* Type of data in terms of the different categories of data, such as non-personal data, personal data, special categories of personal data, data relating to criminal convictions and offenses, data relating to vulnerable persons, highly personal data and sensitive data.
 |
| Automated decision-making | Automated decision-making occurs when personal data are processed mechanically and directly result in a computer-assisted decision, i.e. a decision taken by data processing equipment, which is not subject to even only a partial evaluation or the influence of a natural person. |
| Employees | Employees are defined according to § 26 para. 8 of the Federal Data Protection Act (BDSG) as:* workers, including temporary workers in relation to the hirer,
* individuals employed as part of their vocational training,
* participants in measures for the integration in the labor market and participation in assessments of occupational suitability or trial placements (persons undergoing rehabilitation),
* those employed in recognized workshops for disabled people,
* volunteers performing a service under the Youth Volunteer Service Act or the Federal Volunteer Service Act,
* persons who, because of their lack of economic independence, are to be regarded as persons similar to workers; also including persons employed in homeworking and persons held equal to them,
* federal public employees, federal judges, soldiers and persons performing civilian service,
* job applicants and persons whose employment has ended.
 |
| Biometric data | Biometric data according to Art. 4(14) of the GDPR means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data (e.g. fingerprints). |
| Radio signals | A radio signal is a character or short string of characters emitted by radio waves for the wireless transmission of messages, regardless of the radio technology used, such as mobile radio, radio broadcasting, WLAN, RFID or Bluetooth. |
| Genetic data | Genetic data according to Article 4(13) of the GDPR means personal data relating to the inherited or acquired genetic characteristics of a natural person, which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question. |
| Artificial intelligence | Artificial intelligence is a branch of computer science that deals with systems that exhibit intelligent behavior by making decisions – with a certain degree of autonomy – based on algorithms and machine learning, not only on the basis of existing knowledge, but also by independently expanding their knowledge by evaluating similar problems and their solutions.  |
| Mobile optical-electronic detection | Mobile optical-electronic collection of personal data means any activity intended to observe events and individuals in image and sound at any chosen location, by means of suitable devices and equipment without fixed installation, such as dashcams or camera drones, whether or not subsequent storage of the images or videos takes place or is intended.  |
| New technology | Technology here includes systems consisting of hardware and software, as well as processes and methods of information technology. A technology is new if it is still in the development stage or has only just reached market maturity. Examples include, in particular, applications from the fields of smart cars, smart health, big data and artificial intelligence. |
| Publicly accessible area | A publicly accessible area is an area, which is in fact accessible to an indefinite number of persons and is also intended for this purpose. |
| Profiling | Profiling according to Art. 4(4) of the GDPR means any form of automated processing of personal data making the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. |
| Risk analysis | The risk analysis must identify the risks to the rights and interests of the data subjects resulting from data processing. Risks consider two factors from a data protection perspective: the probability of occurrence and the severity of the damage. Under the ZAWAS process, risk analysis requires the following four steps: * identify risks,
* assess the severity of damage,
* evaluate the probability of occurrence,
* determine the risk score.
 |
| Vulnerable data subjects | Vulnerable data subjects include groups of people who, by virtue of particular characteristics or circumstances, are deemed to be in need of special protection, as well as data subjects in situations where there is a particularly unequal relationship between the position of the controller and that of the data subject.  |
| Scoring | Scoring according to § 31 para. 1 of the German Federal Data Protection Act (BDSG) refers to the use of a probability rating regarding a certain future behavior of a natural person for the purpose of making decisions on the establishment, implementation or termination of a contractual relationship with this person. |
| Systematic monitoring | Systematic monitoring is understood to mean the observation, monitoring or control of data subjects, where this is based, for example, on data collected through networks or on systematic monitoring of areas, including those that are not publicly accessible.EDPB Working Paper 248 identifies several characteristics for classifying monitoring as "systematic":* occurring systematically,
* agreed, organized or methodical,
* carried out within the framework of a general data collection plan,
* taking place within the framework of a strategy.
 |
| Scope of processing | The scope of processing relates to the quantity of the data and the data processing operations and not to the quality. The following factors should be considered in determining the scope of the data: * number of data subjects – either as a specific number or as a proportion of the relevant population,
* data volume and/or the range of data being processed,
* duration or permanence of the data processing, and
* geographical scope of the processing activity.
 |
| Circumstances of processing | The circumstances of data processing describe the detailed modalities and refer to the concrete implementation of the data processing. The following factors should be considered in determining the circumstances of the data processing: * form of collection – direct collection from the data subject or consultation of a third party,
* various processing steps in terms of evaluation, combination, transmission or profiling,
* technical background of the processing, in particular, by means of in-house or external hardware, network connections and software used,
* use of anonymization procedures and deletion routines,
* the involvement of a processor and
* the place of processing, in particular if it is in a third country.
 |
| Controller | The controller, pursuant to Art. 4(7) of the GDPR, is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. |
| Processing (data processing) | Processing, pursuant to Art. 4(2) of the GDPR, is any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. |
| Processing activity | Processing activity is the brief, purpose-oriented description of (usually) several multiple individual processing operations carried out on personal data with a certain continuity over time.  |
| Sensitive data or data of a highly personal nature | The EDPB uses this phrase in WP 248 without providing differentiated and abstract definitions of either sensitive data or data of a highly personal nature. Data are to be included, which are emphasized in the provisions of the GDPR, as well as other categories of data that may increase the potential risks to the rights and freedoms of individuals because they * accompany domestic and private activities,
* affect the exercise of one of the fundamental rights, or
* the violation of the same is accompanied by serious consequences for the everyday life of the data subject.

The following examples are specifically mentioned by the EDPB:* special categories of data pursuant to Art. 9(1) of the GDPR,
* personal data relating to criminal convictions or offenses pursuant to Article 10 of the GDPR,
* the content of electronic communications,
* location data,
* financial data,
* personal documents,
* diaries,
* notes from e-readers equipped with note-taking features ,
* life-logging data, e.g. collected via pedometers or sports watches.

Over and above the explanations provided by the EDPB, sensitive data may be understood as any information, which, is subject in addition to the confidentiality protections under data protection law to special confidentiality protection through social secrecy, professional secrecy or special official secrecy.  |
| Record of processing activities | The record of processing activities is a list of all of a controller’s processing operations, which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, their scope, their circumstances and their purposes, including the information and particulars referred to in Article 30(1)(a) to (g) or Article 30(2)(a) to (d) of the GDPR, and information that is sufficiently detailed, systematized and organized to allow verification of the record provider being in compliance with its obligations.  |
| ZAWAS | ZAWAS was developed at LfD Niedersachsen (State Commissioner of Data Protection of Lower Saxony) and it is a process for selecting appropriate security measures. It describes a holistic method for properly addressing the GDPR requirement to identify the necessary technical and organizational measures.  |
| Combining datasets | Dataset combination is the process of integrating datasets, which originate from different data processing operations and which were conducted for different purposes, into one dataset, e.g. a file. |
| Purposes of the processing | The purpose of the processing is the description of a controller’s aim and reason for carrying out the data processing – that is, why the controller is carrying out the data processing. According to Art. 5(1)(b) of the GDPR, the purposes of the processing must be specified, explicit and legitimate. At various points, the GDPR includes the following abstract examples of processing purposes, which are to be specified by controllers, such as public archiving purposes, scientific and historical research purposes, statistical purposes (Art. 5(1)(b)), performance of a contract (Art. 6(1)(b)), purposes relating to the performance of a task carried out in the public interest or in the exercise of official authority (Art. 6(1)(e)) or for the purposes of preventive or occupational medicine. |

1. Note: The description should be detailed enough to form the basis for the ensuing review process and for any necessary reasoning or explanations provided, and to ensure the transparency of the process in case of audit by the supervisory authorities. [↑](#footnote-ref-1)
2. If the yes/no response does not directly result from the description of the processing activity, the reasons for the response must be stated in order to comply with documentation requirements. [↑](#footnote-ref-2)
3. Note: WP 248 contains explanations of the criteria: p 10 seqq. [↑](#footnote-ref-3)
4. If two criteria are met, this may suggest that a DPIA needs to be performed, which, however, cannot be automatically assumed. It can also be the case that two criteria are met without there being a need to conduct a DPIA. Conversely, it is also possible that a DPIA must be carried out, even though only one criterion has been met. The reviewer will need to reassess this in conclusion (WP248 rev.01, p 12 seqq.). [↑](#footnote-ref-4)
5. A statement of reasons is required, in particular if two or more criteria are met, but it is denied that there is likely a high risk, cf. Art. 29 Group, WP 248 rev.01, p 12 seq. [↑](#footnote-ref-5)
6. Note: The option to omit a DPIA in light of a general impact assessment is not included here, because neither the European nor German legislators have implemented such an assessment pursuant to Article 35(10) of the GDPR to date. Since the LfD Niedersachsen (State Commissioner of Data Protection of Lower Saxony) has not yet published a list pursuant to Article 35(5) of the GDPR, the present review schedule consequently does not contain a corresponding query either. [↑](#footnote-ref-6)
7. Art. 29 Group, WP 248 rev.01, p 16 seq. [↑](#footnote-ref-7)