Big Data and Law

Caldarola / Schrey

2020
ISBN 978-3-406-74393-1
C.H.BECK

not only to establish a corresponding process for this but has also to create the technical prerequisites for such an export of the data of the Big Data application while still treating them as personal data, or to take into account the existence of such possibilities when setting up a Big Data application (privacy by design, Art. 25 GDPR).

6. Right to lodge a complaint

According to Art. 77 GDPR, Big Data subjects also have a right to lodge a complaint with the data protection supervisory authority responsible for the Big Data application if the Big Data subject is of the opinion that the processing of his personal data in the Big Data application is unlawful. In accordance with Art. 13 (2) (d) GDPR, the Big Data subject must be informed of this by the controller responsible for the Big Data application within the framework of the data protection declaration. **440**

Guiding Principle:

If personal data are stored and processed in a Big Data application, the data subjects have the rights according to Art. 15–21 GDPR. Therefore, the processes and technical conditions necessary for the satisfaction of these respective rights are to be created.

III. Records of processing activities according to Art. 30 GDPR

The following table lists the requirements for the procedure directory/records of processing activities for a Big Data application. **441**

Procedure directory (§ 4e sentence 1 BDSG a.F.)	**Records of processing activities (Art. 30 (1) GDPR)**
Name or company name of the responsible entity for the Big Data application as the controller (No. 1). Owners, directors, managing directors or other managers appointed by law or under the company's constitution and persons in charge of data processing (No. 2) Address of responsible entity (No. 3)	Name and contact details of the controller and, if applicable, of the joint controller, of the representative of the controller and of a possible data protection officer (a)
Purposes of data collection, processing or use (No. 4)	Purposes of processing (b)
Description of the groups of persons concerned (Big Data subjects) and the related data or data categories (No. 5)	Description of categories of data subjects and categories of personal data (c)
Recipients or categories of recipients to whom the data may be communicated (No. 6)	Categories of recipients to whom the personal data have been or will be disclosed in or from the Big Data application, including recipients in third countries or international organizations (d).

Procedure directory (§ 4e sentence 1 BDSG a. F.)	Records of processing activities (Art. 30 (1) GDPR)
Planned transfer of data to third countries (No. 8)	If applicable, transfers of personal data to a third country or to an international organization, including the indication of the third country or the international organization concerned, as well as the documentation of appropriate guarantees for the data transfers referred to in Art. 49 (1) GDPR (e).
Standard periods for erasure of data and analysis results related to specific Big Data subjects by the controller responsible for the Big Data application (No. 7)	If possible, the time limits foreseen for the erasure of the different categories of data (f).
General description enabling a preliminary assessment to be made as to whether the measures pursuant to § 9 BDSG a. F. to ensure the security of the processing are appropriate (No. 9); pursuant to § 4g (2) sentence 2 BDSG previous version only for the internal directory.	If possible, a general description of the technical and organizational security measures referred to in Art. 32 (1) GDPR (g)

Figure 62: Record of processing activities

442 Violations of the obligation to draw up and maintain records of processing activities in accordance with Art. 30 GDPR may result in the legal consequences described in mn. 510 *et seq*. below.

443 If third party services are used to operate the Big Data application as processor, the processor shall also maintain a processing directory of this type.

Guiding Principle:
For each Big Data application in which personal data are stored and processed, records of processing activities in accordance with Art. 30 GDPR shall be kept both by the controller responsible for the Big Data application and, where applicable, by the processor.

444 In addition, comparable documentation obligations may also arise for non-personal data, for example if the number and type of use of such data by the data provider is relevant to remuneration.

IV. Implementation of technical and organizational measures to protect personal data from unauthorized access

445 According to § 9 BDSG a. F., the controller responsible for the Big Data application had to adopt the technical and organizational measures listed in the Annex to the BDSG a. F. only in accordance with its protective aims and to examine these regularly to see whether they still met the risk potential to which the raw data, the data records generated in the Big Data application and the analysis results relating to specific Big Data subjects had been exposed.

446 Art. 32 (1) GDPR formulates this requirement much more generally. Accordingly, the controller responsible for the Big Data application has to take appropriate technical and organizational measures, taking into account the state of the art, the implementation costs and the type, scope, circumstances and purposes of the processing as well as the different probability of occurrence and severity of the risk for the rights and freedoms of natural persons, in order to guarantee a level of protection appropriate to the risk. As examples of such measures, some measures are then listed, namely:

- the encryption of personal data,
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of the systems and services associated with the processing,
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and
- a process for the regular testing, assessment and evaluation of the effectiveness of the technical and organizational measures taken to ensure the security of processing.

447 The wording of the regulation differs in many ways from the BDSG a. F.; nevertheless, the principles and considerations developed in § 9 BDSG a. F. and its annex will have to be consulted if one is to envisage the meaning and purpose of Art. 32 GDPR.[128] This results in the following protective goals and the measures listed as examples. Whether and which of these measures are to be taken must then be assessed in each individual case, taking into account the specific technical and structural conditions at the controller responsible for the Big Data application.

1. Access control

448 Unauthorized physical access is to be prevented, whereby the term is to be understood spatially. Measures for entry control, in particular also for the lawful authority of authorized persons include the following:

- designation of authorized persons (internal and external)
- access control system
- access control system such as badge reader, magnetic card or chip card
- register of key holders
- requirements for external persons (visitors, cleaning staff or other external companies)
- attendance records
- visitor badges
- alarm system, factory security or other protective measures outside business hours
- establishment of security zones with access restrictions
- secured supplier entry and exit
- door security (e.g. electric door openers, card readers, TV monitors, security personnel)
- installation of airlocks
- closed data centre operation
- mutual monitoring
- suitable measures for building security (e.g. special glazing, intruder alarm, floor checks, sealing off outlet pipes)

2. (Virtual) Access control

449 Unauthorized access to Big Data applications must be prevented. Measures regarding user identification and authentication must be taken, such as:

- lock function at work stations
- identification of a terminal or user to the Big Data application
- password procedure (e.g. special characters, minimum length, regular password change)
- function-based assignment of individual terminals and identifiers

[128] Cf. Paulus, in: Wolff/Brink, *BeckOK DatenSR*, 25th ed., as at 1.8.2018, Art. 32 GDPR mn. 6.

- functional and/or temporal restrictions on the use of terminals and identifiers
- control of user access rights
- obligation to comply with data secrecy according to § 5 BDSG a. F./Art. 5 (1) (f) GDPR
- use of user codes for files and programs
- use of encryption programs for files and data carriers
- differentiated admission requirements
- guidelines for file organization
- acquisition and analysis of data usage
- specific control over the use of utility programs, where they are likely to circumvent security measures
- controlled destruction of data media
- work instructions and procedures for data acquisition
- control, permission and monitoring systems
- program checks and release processes

3. Admission control

450 Unauthorized activities with or in the Big Data application beyond the granted authorizations must be prevented. Measures for a needs-based design of the authorization concept and access rights as well as their monitoring and logging include in particular:

- work stations with function-bound access keys
- differentiated authorizations (profiles, roles, transactions and objects) including documented authorization concept
- automatic control of access rights, e.g. through identification keys
- keeping access logs
- analysis of access logs
- card reader at the terminal
- time limit for access
- allocation of limited access rights only to certain data or functions
- regular examination whether authorizations granted are still required, cancellation of authorizations for employees who have left the company

4. Data medium control

451 Unauthorized reading, copying, modification or deletion of data media must be prevented. Possible measures for this could be:

- encryption of data media
- locked storage of data media
- tracking the delivery of data media to employees and their return to a locked storage facility

5. Access and user control

452 It must be ensured that those authorized to use the Big Data Application can only access such content, including their evaluations and analysis results, for which they are authorized and that personal data cannot be copied, changed or erased without authorization during processing and use and after storage in the Big Data Application and any previous systems for processing this data. Measures of access and user control may include, among others:

- authorization concept
- user ID with password
- secure interfaces

- data media management
- certificate-based access authorization
- system internal authorization administration
- authorization management by the responsible system administrator

6. Control of disclosure, transmission and transport

453 The following aspects of the disclosure of personal data relating to Big Data subjects shall be regulated: electronic transmission, data transport, transmission control, measures taken during transport, transfer and transmission or storage on data carriers (manual or electronic) and subsequent verification. Such measures may include in particular:

- designation of authorized persons and control of authorization during data transfer by presentation of suitable proofs of authorization
- mutual monitoring
- secured supplier entry and exit
- use of encryption during transmission or tunnel connections (e.g. VPN)
- electronic signature
- inventory checks
- separate, secure storage of data media with confidential content
- access authorization to archived data media
- prohibition on carrying bags or other luggage in restricted areas
- monitoring the destruction of data media and waste materials (e.g. misprints)
- control over the making of data copies
- documentation of data acquisition and transmission programs and data transmission
- documentation of transmission locations and routes
- regulations for packaging and transport of data media (e.g. security containers, personal collection, courier service or accompanied transport)
- encoding
- plausibility and completeness checks
- deletion of residual data before switching data carriers
- remote maintenance concept including access restricting regulations
- tracking of remote maintenance accesses

7. Input and storage control

454 The traceability and documentation of the administration and maintenance of the raw data, the data prepared in the Big Data application and the analysis results related to specific Big Data subjects in the Big Data application must be guaranteed. Measures for subsequent verification as to whether and by whom data have been entered or removed (deleted; erased) can include, in particular:

- documentation of organizational responsibilities for data entry
- obligation to comply with data secrecy
- keeping a protocol of data entries
- maintenance of file usage protocol
- work instructions, process descriptions.

8. Contract control

455 If necessary, C2P, which is to take place only as directed, shall be guaranteed if the controller responsible for the Big Data application uses third parties to operate a Big Data application and/or to maintain it and/or the underlying database management

system – in particular remotely. Measures (technical/organizational) to distinguish the areas of responsibility between the controller and the processor may be in particular:

- clear contract terms
- formalized order placement (order form)
- criteria for the selection of the contractor
- checking the performance of the contract and the contractual performance results
- regular performance of data protection and/or IT security audits by internal or external auditors

9. Availability control

456 The data in the Big Data application must be protected from accidental destruction or loss. Measures for data backup (physical/logical) can include the following, in particular:

- backup procedure
- mirroring of hard disks (e.g. RAID process)
- uninterrupted power supply (UPS)
- early fire detection/smoke detection systems
- protection from smoke in data centres
- protection from water ingress, other water or moisture damage
- redundancy in air conditioning and power supply (including emergency power system and sufficient fuel supply)
- virus protection/firewall
- separate storage
- measures concerning the ageing of data media
- measures relating to archive copies when introducing new releases of the relevant application with which the archived data was created.
- data carrier administration and regular data carrier inventory
- emergency plan

10. Separation control

457 Accordingly, data which were acquired for different purposes are to be generally processed separately, unless an independent lawful basis and the conditions for a change of purpose in Art. 6 (4) GDPR (cf. mn. 230 *et seq.*) exist for their additional storage with other data in the Big Data application in individual cases. Measures for the separate processing (storage, change, erasure, transmission) of data with different purposes can be:

- *internal multi-client capability*/designated purpose
- separation of functions (production/testing/development)

11. Recoverability

458 Measures must be in place which allow systems used for the establishment and operation of Big Data applications can be restored in the event of a disruption. Such measures can be, for example:

- definition of disaster recovery measures depending on the findings of protection requirements
- regular updating of the defined disaster recovery measures
- training of the defined measures with the employees concerned
- regular practice of disaster recovery
- documentation of the results of the disaster recovery exercises and their analysis to effect improvement

12. Reliability

All functions of the Big Data application are to be available and any malfunctions that occur are to be reported. Measures for this could be, for example: **459**

- automatic monitoring of the system, depending on possible protection requirement findings
- implementation of a SIEM system and definitions of actions/reactions to security incidents
- automated reports for compliance, IT security, and senior management

13. Data integrity

Personal data stored in the Big Data application must not be able to be damaged by system malfunctions. Measures for this can be, for example: **460**

- transmission of checksums that indicate whether data has been changed
- Message Authentication Codes to detect both transmission errors and manipulations
- measures, such as acknowledgement messages or sequence numbers, to detect and prevent total loss of messages, unwanted duplication or changes in the sequence of several messages

14. Sanction for non-existent or inadequate technical and organizational measures

Whereas the non-application or inadequate application of technical and/or organizational measures for the protection of personal data within the scope of the BDSG a. F. was not yet punishable as an administrative offence with fines until 24 May 2018, the non-application or inadequate application of technical and organizational measures for the protection of personal data from 25 May 2018 onwards is not permitted. Pursuant to Art. 83 (4) (a) GDPR, a breach of Art. 32 GDPR is an administrative offence that can be punished with fines of up to EUR 10 million or, in the case of a company, of up to 2 % of the total annual turnover generated worldwide in the previous financial year, whichever is greater. **461**

However, there is no risk of criminal liability; the non-application or application of insufficient technical and organizational measures for the protection of personal data is neither a criminal offence within the meaning of § 44 BDSG a. F. nor within the meaning of § 42 BDSG applicable from 25 May 2018. **462**

Guiding Principle:

For a Big Data application, in which personal data are stored and processed, technical and organizational measures according to Art. 32 GDPR are to be carried out and documented.

V. General principles for the processing of personal data in Art. 5 GDPR

1. General principles for the processing of personal data

According to Art. 5 (1) GDPR, personal data must be **463**

- processed lawfully, fairly and in a transparent manner in relation to the data subject (*lawfulness, fairness and transparency*);
- collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes; […] (*purpose limitation*);

- adequate and relevant to the purpose and limited to what is necessary for the purposes for which they are processed (*minimization of data*);
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (*accuracy*);
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (*retention limitation*);
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (*integrity and confidentiality*);

464 Compliance with all these principles, even in the case of Big Data applications, shall be ensured by the controller responsible for processing personal data in the Big Data application (which shall be determined in accordance with the principles set out in mn. 122 *et seq*.). The essential general principles listed in Art. 5 (1) GDPR for the processing of personal data in Big Data applications have already been addressed in one form or another in this guideline, as far as they are relevant in the situation mentioned here.

2. Principle of accountability (Art. 5 (2) GDPR)

465 In view of the large number of data processing operations and their lawful grounds it is important for the principle of accountability laid down in Art. 5 (2) GDPR that the authority be valid via one of the following: declarations of consent (if necessary) pursuant to Art. 6 (1) (a) GDPR, by the balancing of interests (Art. 6 (1) (f) GDPR) or by contracts to be concluded with the Big Data subject (Art. 6 (1) (b) GDPR). According to this Art. 5 (2) GDPR, the controller responsible for the Big Data application is obliged to ensure compliance with the principles in Art. 5 (1) GDPR and must, above all, be able to prove compliance.

3. Sanctioning a breach of these principles

466 A breach of one of the principles of processing of personal data in Art. 5 (1) GDPR, or missing proof for the observance of these principles to be documented pursuant to Art. 5 (2) GDPR, constitute an administrative offence which can be punished by fines; on possible legal consequences, cf. the explanations under mn. 510 et seq. A breach of the accountability principle in Art. 5 (2) GDPR represents a penalty which can involve fines even where the data processing was permissible but only insufficiently documented.