Code of Conduct for the review and erasure time limits in relation to personal data applicable to German credit agencies from 25.05.2018

1. Preamble

The Association “Die Wirtschaftsauskunfteien e.V.” (hereinafter “DW”) represents the interests of large credit agencies.

The companies that have acceded to this code of conduct undertake to comply with it from the date of accession. The company’s accession will be documented by the Association and announced appropriately.

The members include the companies Bisnode Deutschland GmbH, Creditreform Boniversum GmbH, CRIF GmbH, IHD Gesellschaft für Kredit- und Forderungsmanagement mbH, infoscore Consumer Data GmbH, SCHUFA Holding AG and the Verband der Vereine Creditreform e.V.

The purpose of the Association is to combine the interests of the credit agencies through a voluntary association of undertakings and associations of undertakings active in this sector and to promote such interests by setting common goals. The Association represents the interests of its members by putting forward their position to the regulatory authorities of the German federal states, the ministries and political decision makers on issues that are of major importance for the activities of the members.

A further important matter for the Association is the setting of quality standards for the sector. This concerns in particular the area of data protection that has especially high significance for the credit agencies.

The European General Data Protection Regulation (GDPR) will largely supersede the German Federal Data Protection Act (Bundesdatenschutzgesetz or BDSG). When the GDPR comes into force there will lapse i.a. relevant regulations for data processing by German credit agencies. These include the review and erasure periods contained until now in S.35 ss. 2, 2nd sentence no. 4 BDSG (former version). This was intended to ensure a review on the expiry of four or three years of whether longer-lasting storage was required. Ordinarily this would achieve the erasure of facts that had ceased to be relevant. But conversely it was also acknowledged by reason of the periods provided by S.35 ss. 2, 2nd sentence no. 4 BDSG (former version) that in any event storage occurring within those periods is necessary and in the parties ‘interests. The GDPR does retain in Art. 5 (1) (e) the principle of necessity, but does not include any defined assessment periods. But to safeguard effectively the test of necessity, Recital 39 nevertheless assumes that the controller will schedule appropriate time limits.

For clarification it should be noted that erasure on a specified day provided in the following code also includes respectively erasure in the course of the weekend following the deadline.

This code of conduct does not exclude the conduct of a separate review in an individual case at the request of the data subject (under Arts. 17 and 21 GDPR).

In agreement with its members, in the interests of legal certainty in the course of processing data permissibly collated for the purposes of assessing creditworthiness, the DW Association has therefore formulated the list below of periods for review of the need for erasure of personal data stored in master files. The periods set herein establish unified standards and constitute a voluntary commitment on the part of the members to comply with the rules set out in this document and to align with this code of conduct.

The rules of conduct stated herein are intended to guarantee to the data subjects that

in the credit agency sector high importance continues to be placed on data protection concerns after the coming into force of the GDPR from 25.05.2018,

storage of their personal information will conform with data-protection, in that it is geared to necessity, in the course of which the legitimate interests of the data subjects and the controller are reconciled and

there will continue to be transparency for them in relation to the review and erasure periods applied by credit agencies and that in this way processing will be carried out fairly.

The code of conduct stated herein concerns the processing of personal data by the member companies in Germany; they do not contain any declarations concerning storage and erasure periods in the course of the processing of personal data outside Germany.

This code of conduct does not contain any regulations concerning the substantive right to store personal data. The provision of storage and erasure periods is also not indicative of legitimacy of the storage of personal data.

The following storage and erasure periods shall apply regardless of whether the underlying data was collected and stored on a statutory basis or in reliance on consents.

It is intended to broaden the code of conduct gradually to cover further and other issues relevant to data protection law.

2. Review and erasure periods for personal data

2.1. Personal data on receivables due, open and uncontested:

- Personal data on receivables due, open and uncontested shall remain stored for so long as settlement has not been notified; the need for continuing storage shall be reviewed in each case three years (specific date) after the respective event (e.g. first registration of the receivable or account balance update).
- Erasure of personal data shall occur on a specified date three years after settlement of the receivable.
- Notwithstanding this, at the request of the data subject an individual review of whether the storage of the data is still necessary will be carried out (Art. 17 (1) (a)) GDPR).

2.2. Personal data that underlie entries in the record of debtors or publications on (consumer or standard) insolvency proceedings:

- Data from the debtor registers of the central enforcement courts (entries under S.882c para. 1 sentence 1 nos. 1 – 3 German Code of Civil Procedure) shall be deleted precisely three years after entry in the debtor register, or earlier where the credit agency is provided with evidence of or informed of erasure by the central enforcement court.
- Information concerning (consumer or standard) insolvency proceedings or residual debt discharge proceedings shall be deleted precisely three years after the end of the insolvency proceedings or grant of residual debt discharge.

Information concerning

the dismissal of an application for insolvency owing to insufficient assets,

the lifting of protective measures or

the refusal of residual debt discharge

shall be deleted precisely three years later.

2.3. Personal data concerning continuing obligations (contract data), that carry a financial credit risk by reason of an advance payment:

- Information concerning error-free contract data on credit relationships that is documented with receivable based thereon (in particular loans, financial assistance, instalment delivery contracts or part payment) shall remain stored until the open receivable on which they are based is settled; once settlement is notified personal data shall be erased precisely three years thereafter.
- Information concerning error-free contract data on accounts that are documented without the receivable on which they are based (e.g. giro accounts, credit cards, telecommunications accounts or energy accounts) shall remain stored for so long as the accounts exist; once their termination is notified the information shall be erased.
- Information concerning contracts in respect of which there is a statutory provision for evidential review (such as in the case of attachment protection accounts or basic accounts) shall remain stored for so long as they are in existence; once their termination is notified the information shall be erased.
- Information concerning guarantees shall be erased immediately on notification of termination of the guarantee.
- Trading accounts that are conducted in credit shall be erased precisely three years after all receivables have been repaid.

The aforesaid data shall be erased immediately on settlement in accordance with the foregoing provisions on the request of the data subject.

2.4. Other data:

- Previous personal addresses shall remain stored for precisely three years; thereafter there will be a review of the need for continuing storage for a further three years. Thereafter they will be erased on a specific date save where a longer lasting period of storage is necessary for the purposes of identification.
- Information concerning the misuse of an account or a card by the lawful account holder shall be erased after precisely three years.
- Information on dubious or unusual facts that may to be checked and monitored as part of the prevention of money laundering and fraud and fraud prevention and for which the examination shows that not only a mere case of suspicion is given, but that there are sufficient there are reasonable grounds for believing that a money laundering or fraud money laundering or fraud-relevant facts are actually present, are the facts are actually present, the data are collected on a daily basis after three years, starting from the date of the occurrence of the suspicious event.

- Details of enquiries of third parties shall remain stored for at least one year, but at most for three years precisely. On the expiry of one year details of these enquiries must be erased should the data subject so request.
- The necessity of ongoing storage of data taken from other public/publicly accessible sources that contain a personal reference shall be reviewed at the latest after three years. In the case of settlement such as e.g. alteration or deletion in the Commercial Register, erasure of the personal data shall occur after three years.

3. Review of compliance with the erasure periods provided for herein

The companies that accede to this code of conduct guarantee that compliance with the review and erasure periods set herein may be verified at any time. The DW Association shall – irrespective of the tasks and powers of the respective company data protection officer and competent supervisory authorities - nominate for the monitoring of compliance with these rules of conduct a body accredited by the competent supervisory authority in accordance with Art. 41 (1) GDPR. At the option of the DW Association this may be an external body with the required accreditation or an appropriate body from within the DW Association.

3.1. For the monitoring DW shall appoint an inspection body that

has demonstrated its independence and expertise as regards the subject matter of the monitoring to the satisfaction of the competent supervisory authority ;

has demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not give rise to a conflict of interest;

has appropriate financial and staff resources depending on the number, size and complexity of the companies to be monitored and the risk content of the data processing and has demonstrated this to the satisfaction of the competent supervisory authority;

deploys its own staff, not subcontractors, in the performance of the core tasks of monitoring,

has notified the competent supervisory authority of specific contact persons and their contact details for the monitoring;

in so far as it concerns a monitoring body from within the DW Association, its organisational structure up to and including the level beneath the management is separated from the other areas of the Association; DW shall in this case ensure that the internal monitoring body can act independently and is protected from any sanctions in the course of carrying out its tasks.

3.2. The monitoring body tasked with the monitoring of this code of conduct shall carry out the following tasks and duties:

Continuous monitoring and annual rotating review of a suitable number of the acceded companies depending on the risk content of the data processing and identified focal points and eventdriven assessment of the respective acceded company (in particular in the event of complaints relating to alleged non-compliance with this code of conduct by an acceded company).

Regular and event-driven monitoring of the suitability of this code of conduct. This shall include the conceptional examination of whether this code of conduct is practicable, sufficiently precise and formulated comprehensibly and whether it covers the regulatory requirements and is accepted practice.

Event-driven duty to report immediately on the measures taken and their rationale and to the management of the company concerned and to the competent data protection supervisory authority for the company concerned. The monitoring body shall enable a direct reporting channel to the management of the acceded company.

The monitoring body shall have all the investigatory powers necessary to carry out its tasks. The acceded companies shall make available on demand the information required for this. It shall have access to all personal data, processing operations and other information that are required for the performance of its tasks. In addition, the acceded companies shall allow it access to business premises, including all data processing equipment. The monitoring body can also conduct investigations in the form of data privacy inspections. The investigatory powers may be exercised also in relation to external processors of the acceded companies and third parties within the meaning of Art. 4 (10) GDPR.

The monitoring body shall document its monitoring activities and take suitable measures, where necessary, against the acceded companies so that the code of conduct provided herein is complied with and further developed by DW – where such need is identified – in coordination with the competent supervisory authority.

The monitoring body shall take suitable measures in the event of breaches of this code of conduct against the company concerned with the purpose of stopping the identified breach and avoiding its repetition. It will treat as confidential all information concerning companies and natural persons (including data subjects and complainants) and keep such information secret. The monitoring body may pass information to the competent supervisory authority, where this is necessary for the

performance of its tasks and duties. It will inform the management of the company concerned and the competent supervisory authority in the event of detecting breaches of this code of conduct without undue delay of the measures taken and their rationale.

The monitoring body may exclude acceded companies from this code of conduct in the event of repeated breaches or in the case of unremedied detected breaches.

4. Other

Reservation clause

This code of conduct and the monitoring provisions in clause III. shall apply subject to legislative changes affecting their regulatory content or divergent decisions at the European level (European Data Protection Board, European Court of Justice).

Evaluation

This code of conduct shall apply until 25.05.2024. At the latest two years before its expiry the DW Association shall present to the competent supervisory authority a written evaluation report. Where the supervisory authority raises no objections, this code of conduct shall extend for a further six years.