melissa

A **MELISSA** WHITEPAPER

Quite Good Friends: Data Quality and General Data Protection Regulation

From obligation to opportunity: How you can not only comply with the GDPR with high data quality, but also increase your profit.

TABLE OF CONTENTS

The General Data Protection Regulation (GDPR) has been in effect since 2016. After a two-year transition period, all EU Member States must implement it. Yet companies are still confronted with taking technical and organizational measures to meet the high requirements for data protection and avoid penalties. Numerous legal proceedings in which companies were sued for not processing or storing personal data in accordance with the GDPR show that not every organization can do this in full.

According to the Enforcement Tracker Report by the law firm CMS, European data protection authorities have become active in more than 1,500 cases since the GDPR came into force and have imposed fines of 1.19 billion euros in the past twelve months alone.[1]

THE PURPOSE OF THE GDPR

In short, the GDPR is primarily about protecting personal data from unwanted spying and misuse. In addition, since the introduction of the GDPR, individuals have rights regarding the storage and use of their data. The regulation does not distinguish whether they are stored in analogue or digital form.

WHAT IS PERSONAL DATA?

The European Commission has published the following definition: "Personal data is all information that relates to an identified or identifiable living person. Various pieces of information, which together can lead to the identification of a specific person, also constitute personal data. Personal data that is anonymized, encrypted or pseudonymized but can be used to re-identify a person remains personal data and falls within the scope of the General Data Protection Regulation."[2]

[1] **https://www.onetoone.de/artikel/db/772501gehl.html**
[2] **https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_de**

HIGH DATA QUALITY IS ESSENTIAL TO BEING GDPR COMPLIANT

In Article 5(1)(d), the GDPR stipulates that personal data must be correct. Specifically, it says: "Personal data must be objectively correct and, if necessary, be up to date; all reasonable measures shall be taken to ensure that personal data that is inaccurate with regard to the purposes for which it is processed is deleted or corrected without delay ("correctness")."

For this reason, companies are required to ensure the highest quality of their stored personal data. The data quality can be evaluated on the following criteria:[3]

CORRECTNESS: The data must match reality.

CONSISTENCY: A data set must not have any contradictions in itself or with other data sets.

RELIABILITY: The origin of the data must be traceable.

COMPLETENESS: A data set must contain all necessary attributes.

ACCURACY: The data must be available with the required level of accuracy.

CURRENTNESS: All data sets must correspond to the current state of reality.

REDUNDANCE-FREE: No duplicates may occur within the data records.

RELEVANCE: The information content of data sets must meet the respective information requirements.

UNIFORMITY: The information in a data set must be uniformly structured.

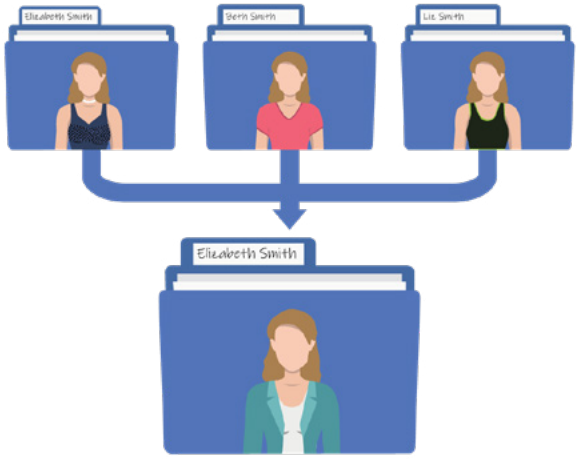
UNIQUENESS: Each data set must be ambiguously interpretable.

COMPREHENSIBILITY: The data sets must correspond in terms and structure with the expectations of specialized departments.

[3] **https://www.computerwoche.de/a/gute-daten-schlechte-daten,1931857**

WHAT FACTORS NEGATIVELY AFFECT DATA QUALITY?

It is not easy to ensure that these criteria are met on an ongoing basis. This applies in particular to the currentness of the data. According to a recent study by Deutsche Post, every eighth customer address in databases of German companies is incorrect.[4] Reasons for this are mainly moving house and deaths, followed by serious errors in street and place names, as well as postal codes and house numbers. Changes in marital status also mean that data is no longer up to date.



If companies retain such outdated or incorrect data, they generally violate Article 5(1)(d) of the GDPR ("correctness"). In addition, they cannot easily comply with Article 17 ("right to be forgotten"), as they simply cannot find the respective data sets. Similar mishaps can happen if the data is stored redundantly in different systems. For example, it is often the case that Sales work with saved contact details in the Customer Relationship Management (CRM) system, while invoices are issued to addresses saved in the Enterprise Resource Planning (ERP) system. In addition, there are contact details that prospective customers have entered on the website to, for example, subscribe to a newsletter or to request further product information. For companies, it is then almost impossible to delete the personal data of "John Doe" if it is listed in different systems under "John Doe", "Doe John" and "Mr. Doe". The risk is high that the data will only be deleted once. In this case, the data subject would continue to receive correspondence and could take legal action against the responsible company.

[4] **https://www.dpdhl.com/de/presse/pressemitteilungen/2023/deutsche-post-direkt-adress-studie-2023.html**

TECHNICAL MEASURES TO INCREASE DATA QUALITY

In order for companies with high data quality to meet the requirements of the GDPR, they must, above all, carry out data management correctly. "Correct" in this context means most importantly that the data is stored in a structured manner in a system. This requires breaking down the data silos created in the past and consolidating personal data.

Define a single point of truth

For this purpose, those responsible should first define which system acts as a master, so to speak, a single point of truth, and thus forms the basis for correct data in the future. Whether this is the CRM or the ERP solution depends on individual processes.

Identify the golden record

In the next step, the data contained therein is checked and cleaned up, i.e., sort out any inactive accounts. Carried out manually, this work requires a disproportionate amount of effort. Solutions that automatically validate contact details are more cost-effective and quicker. Then the company would identify what additional data might be stored in its other systems. These too must first be validated and duplicates removed. As a result, the accurate data is consolidated in a system, which leads to the golden record. This lays the foundation for ensuring high data quality.

Implement autocomplete

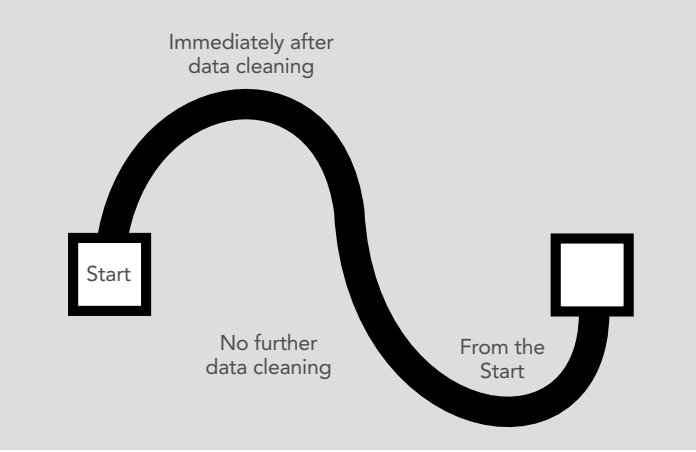
So that incorrect or duplicate records are not added again, it makes sense to use an autocomplete directly at the point of entry. Such solutions act as guards so that false data has no chance of entering the system. In addition, this leads to a better customer experience, because the shopping experience is improved with the help of an automatic completion of the entered data. The basis for this is a standardized database with valid place and street names.

The customer only needs to enter the first few letters and immediately receives suitable suggestions. Experience has shown that this halves the keystrokes and the associated risk of incorrect entries. In addition, the collection of address data is accelerated, so that the customer can complete their order much faster.

Another aspect is the so-called "Google mentality" of the internet-savvy and affluent generations X, Y and Z. Users do not want to waste time typing whole addresses into a form but prefer it if the tool makes qualified suggestions. On the provider side, this approach has the advantage that the entered contact data can be checked in real time so only validated information can enter the master system. Powerful solutions verify titles, names, streets, postal codes, e-mail addresses and telephone numbers.

Perform regular validations

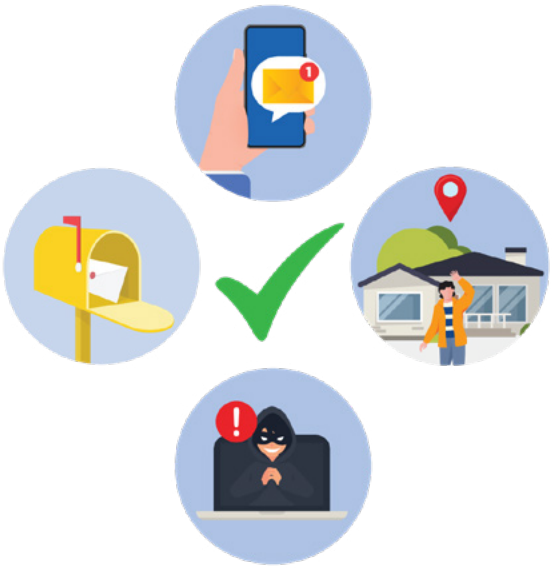
Since, as already explained, customer data can change, it is necessary – in addition to the initial validation – to check it regularly. However, if companies only check the data periodically, for example once per quarter, then their quality corresponds to a sine curve. The quality is high immediately after the data cleaning and falls until the next cleansing, only to rise again. In contrast, software solutions continuously validate the existing entries with current reference data.



OTHER ADVANTAGES OF HIGH DATA QUALITY

High data quality not only simplifies compliance with the GDPR, but also brings the following advantages:

- **Declining costs:** Poor data quality costs money, as shown for years by the 1-10-100 rule of thumb. It costs an average of 1 euro to verify customer master data during initial data entry with the help of professional software support. This amount increases to 10 euros per data record if the data is only cleaned up from time to time in order to correct originally incorrect entries and eliminate duplicates. There is a cost of about 100 euros per data record if a company completely neglects the address quality and does nothing at all.
- **Lower return rate:** With correct customer data, postal items can be delivered reliably and faster. This enhances the customer experience.



- **Improved decision-making:** High-quality data reduces the risk of making incorrect decisions. At the same time, potential effects are more predictable.
- **Better market and target group segmentation:** High data quality allows companies to carry out well-founded market and target group segmentations. This leads to potential new customers and the development of new markets. This means that companies are one step ahead of the competition.
- **Effective marketing campaigns:** In addition to improving segmentation, companies can use qualitative data to learn more about their target group and thus create personalized offers or campaigns.

HOW CAN MELISSA SUPPORT THE IMPLEMENTATION OF THE GDPR?

Even today, the majority of German companies are struggling to fully implement the GDPR in the field of data management.[5] Our reliable, data protection-compliant solutions for autocomplete, address and duplicate checking help to increase data quality and keep it at a high level. Our experts have already supported numerous companies in implementing the requirements of the GDPR sustainably. In our work, we receive professional support from external data protection officers, including the renowned law firm Kinast, which specializes in national data protection.

On the following page, you can read some guest remarks by Dr. Karsten Kinast, LL.M of KINAST Rechtsanwaltsgesellschaft mbH, our external data protection officer. We sign an order processing contract with all of our customers in accordance with the GDPR and develop corresponding technical and organizational measures. In addition, we have the necessary certifications and rely on certified data centers when hosting our web services. In this way, we ensure that our services meet the highest security standards.

[5]https://www.bitkom.org/Presse/Presseinformation/Datenschutz-setzt-Unternehmen-unter-Dauerdruck

As a law firm specializing in data protection law, we, KINAST Rechtsanwälte (www.kinast.eu), have been working with Melissa Data GmbH for many years in the function of its external data protection officer. In addition to Melissa's own obligation to implement the GDPR as a European company, we note one thing above all:

The demand of customers responsible for data protection law for different aspects of data protection at Melissa as a service provider is (quite rightly) very high. After all, the services of Melissa Data GmbH are "Order processing in the core business", in which well-known customers entrust personal data of their legal area of responsibility to Melissa's specialists and system solutions. For this reason alone, Melissa attaches great importance in its work on data protection law to putting the data protection interests of customers in the foreground and to justifying the trust placed in Melissa as a service provider or "processor".

But not only the legal framework conditions are GDPR-relevant: As we understand it, the core of the products and services themselves enable the implementation of data protection law for Melissa customers. The technical-organizational protection goals of the EU regulation with heavy fines include the integrity, availability and confidentiality of data. According to our diverse practical experience, the above-mentioned integrity is very much underestimated and often neglected! However, as well as the much better-known "availability" (backups, fast accessibility) and "confidentiality" (e.g. protection against unauthorized access), data integrity is nevertheless an indispensable cross-sectional competence for the implementation of the GDPR requirements.

"Data integrity is often an underestimated and neglected GDPR requirement!"

Data integrity is about the quality and accuracy of the data itself as well as the correct functioning of systems and databases in which it is processed. So if you investigate a large part of the violations of the GDPR and the so-called "data breaches", the source of the problem is often exactly here. In a loss of control over the uniformity of storage, the accuracy of the processed content on the basis of typos or different writing methods, about the currentness of the data over time and all the resulting consequential errors.

Not infrequently, a lack of data quality and integrity grows into poorly, incorrectly or incompletely answered requests for information from data subjects, not technically effectively implemented advertising opt-outs, unimplemented deletion routines or deletion requests from customers due to duplicate accounts or shows up in the incorrect sending of sensitive content to unauthorized third parties due to incorrect postal or digital addresses, or even mistaking someone for someone else. This can subsequently end with the obligation to report a data protection breach to the data protection supervisory authority as well as claims for damages and fines.

Against this background, our clients are encouraged to understand "data integrity", "availability" and "confidentiality" as an interacting triad and to ensure through technical-organizational measures that neglecting one of the three elements and thus the potential for significant impact on the company's GDPR compliance can be avoided. In addition to economic aspects, Melissa's solutions are thus successfully aimed at ensuring essential elements of GDPR compliance.

- **Dr. Karsten Kinast, LL.M.**
  KINAST Rechtsanwaltsgesellschaft mbH
  External Data Protection Officer of Melissa Data GmbH

www.melissa.de

About Melissa

Melissa is a leading provider of data quality, identity verification and address management solutions. Melissa supports companies in customer acquisition and retention, validating and correcting contact data, optimizing marketing ROI and managing risk. Since 1985, Melissa has been a reliable partner for companies such as Mercury Insurance, Xerox, Disney, AAA and Nestlé in improving customer communication.

Germany

Cäcilienstr. 42-44
50667 Köln

+49 (0) 221 97 58 92 40

U.S.

1 800 MELISSA (635 4772)

CANADA

1 800 635 4772

INDIA

+91 (0)80 4854 0142

UK

+44 (0)20 7718 0070

AUSTRALIA

+61 02 8091 6000

SINGAPORE

+65 8 2997442