

Personal Data Breach Handling Policy

Group Data Privacy

|  |  |
| --- | --- |
|  |  |
| Handling of data privacy incidents |  |
| Number | [Number] |
| Issued on | 21.06.2022 |
| Through | Group Data Privacy Officer |
| Entry into force | 21.06.2022 |
| Scope of application | SÜDVERS Holding GmbH & Co. KG and its majority-owned subsidiaries, as well as SÜDVERS International GmbH |
| Topic | Compliance |
| Responsible function | Group Data Privacy |
| Responsible person | Udo Strittmatter |
| Overriding regulation | SÜDVERS data protection policy |
| Replaces | n/a |
| Applicable documents |  |
| Validity | Until further notice |
| Last review | 25.06.2025 |
| Next review | 07.01.2026 |
| Publication | SÜDVERS Intranet |
| Classification | Internal |
| Archive | Document management system |
| Organizational system | [Organizational system] |
| Languages | English |
| Formats | Online |
| Remarks |  |

Table of contents

[1 Principles 4](#_Toc145062439)

[2 Objectives 4](#_Toc145062440)

[3 Controls 4](#_Toc145062441)

[3.1 Identification and classification 5](#_Toc145062442)

[3.2 Containment and recovery 5](#_Toc145062443)

[3.3 Assessment of risks 6](#_Toc145062444)

[3.4 Notification of violations 7](#_Toc145062445)

[3.5 Process description 8](#_Toc145062446)

[3.6 Checklist regarding reporting obligations 9](#_Toc145062447)

[3.7 Evaluation and reaction 10](#_Toc145062448)

# Principles

A process must be established to govern the handling of personal data breaches to ensure that all regulatory, legal and SÜDVERS internal requirements are met.

# Objectives

SÜDVERS must take appropriate measures against unauthorized or unlawful processing and against accidental loss, destruction or damage of personal data.

# Controls

Personal data breaches can occur for a number of reasons, including, for example

* the disclosure of confidential data to unauthorized persons;
* improper disposal of documents where personal data is deposited in a garbage can accessible to the public;
* Loss or theft of data or devices on which data is stored;
* Loss or theft of paper documents;
* inappropriate access controls that allow unauthorized use of information;
* Suspected violation of SÜDVERS information security and the associated guidelines;
* Attempts to gain unauthorized access to computer systems, e.g. by hacking;
* viruses or other security attacks on systems or networks of SÜDVERS IT equipment;
* Violations of physical security;
* confidential information that remains unlocked in accessible areas; and
* Emails with personal information sent to the wrong recipient by mistake.

However, in the event that a data breach has occurred, there are five important steps for dealing with personal data breaches:

* Identification and classification
* Containment and recovery
* Risk assessment
* Notification of the breach
* Evaluation and reaction

## Identification and classification

SÜDVERS must define and operationalize processes and procedures that enable all SÜDVERS employees to report information/data security breaches and that ensure that all SÜDVERS employees know to whom to report such a personal data breach. The establishment of such processes and procedures will support the early detection of personal data breaches so that they can be dealt with in the most appropriate manner.

Details of (potential) breaches must be accurately recorded, including:

* the date and time of the violation;
* the date and time at which it was discovered;
* who/what reported the violation;
* Description of the infringement;
* Details of all affected IT systems
* other probative material.

All persons at SÜDVERS involved in the handling of personal data breaches must be aware of what constitutes a data breach and what can be defined as a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data that is transmitted, stored or otherwise processed.

## Containment and restoration

Data breaches require not only an initial response to investigate and contain the situation, but also a recovery plan that includes mitigation where appropriate. This often requires the involvement of professionals from across the organization, such as IT, HR and Legal, and in some cases, contact with external stakeholders and suppliers.

If a breach of the protection of personal data has occurred, SÜDVERS

* determine who at SÜDVERS will lead the investigation of the breach and SÜDVERS management must ensure that the responsible person has the appropriate resources;
* Determine the channels of communication related to the breach and inform the parties involved what is expected of them to assist with containment;
* check whether SÜDVERS can do anything to make good any losses and limit the damage that the breach may cause;
* document details of the facts relating to the breach, its impact and the remedial action taken in a SÜDVERS internal personal data breach register; and
* Inform the police if necessary.

## Assessment of the risks

Some data security breaches do not result in risks beyond potential inconvenience to those who need the data for their work. An example would be if a laptop is damaged beyond repair but the files have been backed up and

can be restored, even if this involves certain costs for the company. While these types of incidents can still have significant consequences, the risks are very different than, for example, the theft of a customer or employee database whose data could be used for identity fraud. Before deciding what steps are required beyond immediate containment, you should assess the risks that could be associated with the breach. Perhaps most importantly, assess the potential adverse consequences to the individual, how serious or significant they are, and how likely they are.

When assessing the risk arising from the breach, SÜDVERS must take into account the possible adverse consequences for the individual. When assessing the risk, SÜDVERS must consider the following:

* What type of data is involved?
* How sensitive is it?
* In the event that data is lost or stolen, are there any protective measures such as encryption?
* What happened to the data?
* Regardless of what has happened to the data, what could the data reveal about the person in question to a third party?
* How much personal data of individuals is affected by the security breach?
* Who are the people whose data has been misused?
* What damage can these people suffer?

## Notification of violations

All personal data breaches must be reported immediately to SÜDVERS' Data Protection Officer and an incident report must be prepared containing at least the following information

* Date on which the incident was discovered;
* Date(s) of the incident;
* The scene of the action;
* Name of the person reporting the incident:
* Contact details of the person reporting the incident (e-mail address, telephone number);
* Brief description of the incident or details of the lost information;
* Number of persons affected, if known;
* Brief details of the personal data (possibly) concerned; and
* Brief description of the measures taken at the time of discovery.

Depending on the nature of the personal data breach, notifying individuals, organizations and supervisory authorities that SÜDVERS has suffered such a personal data breach is an important element that may also be required by applicable local data protection laws. However, informing individuals about a data breach is not an end in itself. Notification should have a clear purpose, whether it is to enable the individuals who may have been affected to take action to protect themselves or to enable the relevant supervisory authorities to carry out their duties, provide advice and handle complaints.

The following considerations will help you decide on the best approach to reporting:

* Are there any legal, statutory or contractual requirements?
* Can the notification help SÜDVERS fulfill its security obligations with regard to all applicable data protection regulations?
* Can the notification help the individual?
* How can the notification be designed appropriately for certain groups of people?
* Beware of the risk of "over-notification".

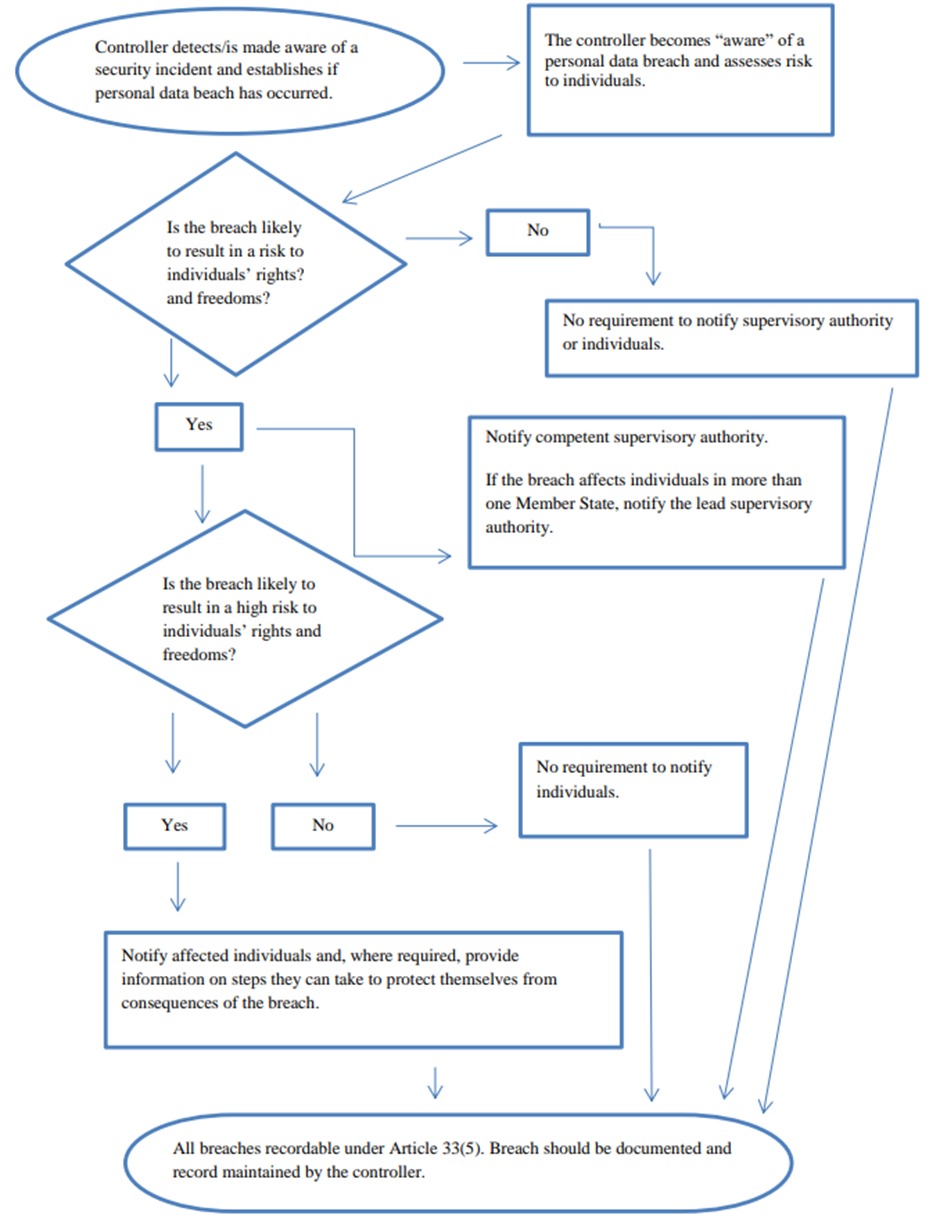
## Process description

The operational process for handling data protection incidents must meet the requirements of the following NIST-800-61 Rev. 2 and EU WP29 compliant business processes:

|  |  |
| --- | --- |
| "Identify and Classify": | "Contain and Recover: |
| "Assess the risks": | "Notify: |
| "Evaluate and Respond": |  |

## Checklist regarding reporting obligations

To check whether a reporting obligation exists, the following information chart in accordance with WP250rev.01 of the Article 29 Data Protection Working Party should be used:



In the event that notification of a data breach is required, consideration must also be given to who is to be notified, what is to be said and how the message is to be transmitted.

* Make sure that you inform the competent supervisory authority and other necessary external parties.
* The notification must be made within 72 hours of the personal data breach.
* The notification must contain at least a description of the following points
  + how and when the violation took place;
  + which data is involved;
  + what SÜDVERS has already done to respond to the risks caused by the breach; and
  + Details of the technical security measures (e.g. encryption)
  + and details of the security procedures in place at the time of the breach
* When notifying individuals, specific and clear guidance must be given on what steps they can take to protect themselves and what SÜDVERS is prepared to do to help them;
* Provide a way for them to contact SÜDVERS for more information or to ask SÜDVERS questions about the incidents;
* There are various ways of notifying those affected, so you should choose the most appropriate one. Always consider the safety of the medium and the urgency of the situation; and
* When informing the media, it makes sense to let them know whether SÜDVERS has contacted the supervisory authority and what measures are being taken.

## Evaluation and response

It is not only important to investigate the causes of the breach, but also to evaluate the effectiveness of SÜDVERS' response to the breach. If the breach was caused, even if only in part, by systemic and persistent problems or by inadequate policies, processes or procedures, then it is not acceptable to simply contain the breach and continue "business as usual".