Data Breach Policy

Policy N°: AEU-LEG-Data Breach Policy–2025

Subject: Data Breach Policy

Version: Final

Approval status: Approved

Effective Date: 2025.6.2

Publication Date:2025.6.2

A. Scope and purpose

Advantech is committed to protecting Personal Data in compliance with the General Data Protection Regulation (***"the GDPR"***) which requires Personal Data to be processed in a manner to ensure appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to Personal Data.

This Policy sets out the guidelines that Company uses to deal with a data breach in a way that allows detecting and promptly containing a breach, to assess the risk to individuals, and then to determine whether it is necessary to notify the competent supervisory authority and to communicate the breach to the individuals concerned when necessary.

This Policy is available and applies to all persons within the Company and adherence to it is mandatory.

B. Definitions

For the purposes of this Policy:

"Advantech" or ***"Company"*** means Advantech Europe B.V. and its controlled Group Companies in Europe;

"Advantech Europe B.V." means the legal entity incorporated in the Netherlands that has overall control over the Group Companies and is presumed to be the decision-making center relating to the processing of Personal Data, and the main establishment for the group, except where decisions about the purposes and means of processing are taken by another establishment.[1];

"***controller***" means 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; where the

[1] GDPR Recital (127) provides for the possibility of local oversight in specific cases ("*Each supervisory authority not acting as the lead supervisory authority should be competent to handle local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involves only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees' Personal Data in the specific employment context of a Member State*.")

purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

"***processor***" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

"***recipient***" means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by [them] shall be in compliance with the applicable data protection rules according to the purposes of the processing;

"Group Companies" means a group of undertakings of branch type or company structure, operating in the Member States of the EU, having Advantech Europe B.V. as a centralized decision-making headquarters in most of operational areas;

"**Personal Data**" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"*Personal Data Breach*" or ***"Breach"*** is a type of a security incident that leads to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed. Unauthorized or unlawful processing may include disclosure of Personal Data to (or access by) recipients who are not authorized to receive (or access) the data or any other form of processing which violates the GDPR (hereinafter: "Breach").

C. Identification of a Breach

i. Detecting and addressing the Breach

As a controller, Advantech ensures that it has appropriate technical and organizational measures in place for an appropriate level of security of Personal Data, taking into account the state of the art, the costs of implementation and the nature, the scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

In order to detect the Breach, the mentioned measures include but do not limit to tracking and analyzing logs and data flows, ongoing employee trainings, following suspicious activity or unauthorized IP addresses on wireless networks.

Advantech also has in place arrangements with processors, which determine obligations for processors to put in place suitable measures to be able to prevent, react and address a Breach and to notify the controller in the event of a Breach.

When addressing the Breach, Advantech makes sure that once a Breach or a suspicion of a Breach is detected, it is reported to the Data Protection Officer (DPO) who is a person with operational responsibility within the Company for managing a Breach. No member of staff should fail to report a suspected breach or attempt to deal with a suspected breach without first speaking to the DPO.

The Data Protection Officer will then address the Breach further by establishing the existence of the Breach and assessing the risk. The DPO will liaise with senior management or relevant IT staff in respect of these issues as appropriate. In cases of data breaches, the Data Protection Officer is responsible for carrying out a full investigation, appointing the relevant staff to contain the Breach, recording the Breach on the breach form, and making any relevant and legal notifications to the supervisory authority, or the affected individuals.

ii. Containing and Documenting the Breach

At the same time as the Breach has been detected, remedial measures must be taken to contain the Breach. Such remedial measures are not in the scope of this document due to the vast nature of breaches and the variety of measures to be taken. As with any security incident, our remedial measures will be based on the Company's investigation on whether the Breach was a result of human error or a systemic issue and see how it can prevent recurrence. Since human error is the leading cause of data breach incidents, we proactively attempt to reduce such risk by implementing the following:

- mandatory employee data protection induction and refresher training; and
- Implementing a culture of trust – employees should feel confident to report incidents or near misses.

The aim of any such measures is to stop any further risk/breach to the organization, customer, client, third party, system or data prior to investigation and reporting. The measures taken are noted on the incident record in all cases.

The Company utilizes a Data Breach Log for all data breaches, which is completed for any data breach, regardless of severity or outcome. Completed forms are logged in the Breach Incident Folder and reviewed against existing records to ascertain patterns or reoccurrences. The completing of the Data Breach Log is only to be actioned after containment has been achieved.

A full investigation is conducted and recorded on the incident form, with the outcome being communicated to all staff involved in the Breach, in addition to senior management. A copy of the completed incident form is filed for audit and record purposes.

D. Assessing the risk

On establishing and becoming aware of a Breach, the DPO is required to assess potential adverse consequences for the individuals whose Personal Data are involved, how serious or substantial these are and how likely they are to happen.

In general, the DPO should ascertain what information was involved in the Breach and what subsequent steps are required to remedy the situation and mitigate any further breaches. The DPO will either lead, or assign an individual to lead, the investigation of the Breach, which shall include an assessment of risk.

When assessing the risk that resulted from a Breach, Advantech will consider the specific circumstances of the Breach, including the severity of the potential impact and the likelihood of this occurring. To complete such assessment of risk, the DPO or lead investigator should consider the following criteria:

CRITERIA	DESCRIPTION
1. The type of breach	a. "*Confidentiality breach*" - where there is an unauthorized or accidental disclosure of, or access to, Personal Data. b. "*Integrity breach*" - where there is an unauthorized or accidental alteration of Personal Data. c. "*Availability breach*" - where there is an accidental or unauthorized loss of access to, or destruction of, Personal Data.
2. The nature, sensitivity, and volume of Personal Data	The more sensitive the data, the higher the risk of harm will be to the people affected, but consideration should also be given to other Personal Data that may already be available about the data subject. Breaches involving health data, identity documents, or financial data such as credit card details, can all cause harm on their own, but if used together they could be used for identity theft. A combination of Personal Data is typically more sensitive than a single piece of Personal Data
3. Severity of consequences for individuals	Severity will depend on the nature of the Personal Data involved in a breach, for example, special categories of data, the potential damage to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation.
4. Special characteristics of the individual and the controller	A breach may affect Personal Data concerning children or other vulnerable individuals. Also, the nature and role of the controller and its activities may affect the level of risk to individuals as a result of a breach.
5 The number of affected individuals	Generally, the higher the number of individuals affected, the greater the impact of a breach can have.
7. Ease of identification	Depending on the circumstances, identification could be possible directly from the Personal Data breached with no special research needed to discover the individual's identity, or it may be extremely difficult to match Personal Data to a particular individual

These criteria will help to assess the probability of the threat occurring as well as the severity/seriousness of the potential impact on the rights and freedoms of individuals.

The likelihood of the threat will be classified as:

1. **Low**: the threat is *unlikely* to materialize.
2. **Medium**: it is *possible* that the threat materializes.
3. **High**: the threat is *likely* to materialize.

The severity of the potential impact will be classified as follows:

LEVEL OF SEVERITY	DESCRIPTION
Low	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, etc.).
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, worsening of health, etc.).
Very high	Individuals may encounter significant or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Taking into account the listed criteria and the determined grade of likelihood and severity of the impact to individual's rights, Advantech will assess the risk and categorise the Breach as High, Medium or Low risk.

		IMPACT LEVEL		
		Low	Medium	High / Very High
Threat Occurrence Probability	Low			
	Medium			
	High			

Legend

Low Risk *Medium Risk* *High Risk*

Clearly, where the consequences of a Breach are more severe, the risk will be defined as higher and similarly where the likelihood of these occurring is greater, the risk is also heightened.

The assessment of the risk will help to determine whether notification is required to the supervisory authority (see point E.) and, if necessary, to the individuals concerned (see point F.).

E. BREACH NOTIFICATIONS – LEAD SUPERVISORY AUTHORITY

The Company recognizes the obligations to report data breaches in certain instances. Key staff have been made aware of the Company's responsibilities and we have developed strict internal reporting lines to

ensure that data breaches falling within the mandatory notification criteria are identified and reported without delay.

Once the Breach is established by the DPO and the risk is assessed, the DPO will decide if it is a notifiable Breach. In case of any breach where it is likely to result in a risk to the rights and freedoms of individuals a notification will be sent without undue delay, and where feasible, not later than 72 hours after becoming aware of the Breach.

The Lead Supervisory Authority for the Company is to be notified of any breach where it is likely to result in a risk to the rights and freedoms of individuals. These are situations which if the breach was ignored, it would lead to significant detrimental effects on the individual. The Lead Supervisory Authority for the Company is the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) since Advantech Europe B.V. is presumed to be the decision-making center relating to the processing of Personal Data, and the main establishment for the group.

In case of joint controllership of Advantech Europe B.V. and another Group Company, the Lead Supervisory Authority will also be the Dutch Data Protection Authority while the joint controllership agreement will further specify their respective responsibilities for compliance with the GDPR.

Where applicable, the Lead Supervisory Authority is notified of the breach no later than 72 hours after the Company becomes aware of such breach and are kept notified throughout any breach investigation, being provided with a full report, including outcomes, and mitigating or remedial actions as soon as possible, and always within any specified timeframes.

If for any reason it is not possible to notify the Lead Supervisory Authority of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for any delay. Where a breach is assessed by the DPO and deemed to be unlikely to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the Lead Supervisory Authority in accordance with Article 33 of the GDPR.

The notification to the Supervisory Authority will contain:

1. Name and contact details of our Data Protection Officer and/or any other relevant point of contact
2. Description of the nature of the Personal Data breach including where possible, the categories and
3. Approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;
4. Description of the likely consequences of the Personal Data breach;
5. Description of the measures taken or proposed to be taken by the controller to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the above information at the same time, such information will be provided in phases without undue further delay.

Breach investigation is always carried out, regardless of our notification obligations and outcomes and reports are retained to be made available to the Lead Supervisory Authority if requested.

Where the Company acts in the capacity of a processor, we will ensure that controller is notified of the Breach without undue delay. In instances where we act in the capacity of a controller using an external processor, we have a written agreement in place to state that the processor is obligated to notify us without undue delay after becoming aware of a Breach.

F. BREACH NOTIFICATIONS – DATA SUBJECTS

When a Breach is likely to result in a high risk to the rights and freedoms of natural persons, Advantech will always communicate the Breach to the data subject without undue delay, in a written, clear and legible format. The notification will contain at least the same content as the one sent to the Lead Supervisory Authority. The notification will also be made in close cooperation with the Lead Supervisory Authority.

Existence of high risk will be assessed by the DPO using the criteria described in point D. of this Policy. DPO may also take into account the relevant provisions of GDPR determining that the risk is high when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves Personal Data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, such damage should be considered likely to occur.

However, our obligation to notify data subject(s) is limited and subject to the following:

> *We reserve the right not to inform the data subject of any Personal Information breach where we have implemented the appropriate technical and organizational protection measures which render the data unintelligible to any person who is not authorized to access it (i.e., state-of-the-art encryption data masking etc.) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialize.*

Additionally, if informing the data subject(s) of the Breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.

G. RECORD KEEPING

All records and notes taking during the identification, assessment and investigation of the Breach are authorized by the Data Protection Officer and are retained for a period of 6 years from the date of the

incident. Incident forms are to be reviewed monthly to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring.

H. RESPONSIBILITIES

The Company will ensure that all staff are provided with appropriate training and support to learn, understand, and implement all procedures within this document, as well as ensuring that employees understand their responsibilities in the breach incident reporting process. The Data Protection Officer is responsible for regular compliance audits and gap analysis monitoring and the subsequent reviews and mitigation/remedial action follow-ups.

I. Validity and document management

This document is valid as of 2025.6.2.

The owner of this document is Data Protection Officer, who must check and, if necessary, update the document at least once a year.

RTA van Velzen

CM&D Director Europe

02/06/2025