Personal Data Breach Management Policy

Effective date: 01.01.2019.

1. Purpose

DPC Consulting Kft. (hereinafter referred to as: the '**Controller**' or the '**Company**') has concluded this policy based on interpretation of the General Data Protection Regulation (hereinafter referred to as: '**GDPR**') and the relevant European Union and national legislation. This policy ensures immediate handling of any possible breach of personal data security to maximise data security, including the documentation of compliance with the relevant legal obligations.

This policy outlines the procedures to follow for the Controller to consistently and effectively address breaches of personal data security or the suspicion of such, that is, the personal data breaches.

The purpose of this policy is to minimize risk in case a data security breach occurs, furthermore, includes the steps to be taken in case of personal data breach and to prevent future infringements.

2. Scope

This policy applies to all personal and special (sensitive data) data categories, regardless of their form.
This policy applies to all employees, subcontractors and clients of Controller. This includes ad hoc employees acting on behalf of Controller, temporary collaborators, contractors or consultants and those hired through agencies.
This policy applies to both suspected and realized personal data breaches.

3. What is a personal data breach?

A personal data breach is an event or act that occurs in connection with this policy, which accidentally or deliberately endangers or violates security of systems or data, that is, their confidentiality, integrity, availability and damage, or may potentially damage the Data Controller's information, tools, and / or reputation.

In its Opinion 03/2014 on breach notification, WP29 explained that breaches can be categorized according to the following three well-known information security principles:
"Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.
"Integrity breach" - where there is an unauthorised or accidental alteration of personal data.
"Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

It should also be noted that, depending on the circumstances, a breach can concern confidentiality, integrity and availability of personal data at the same time, as well as any combination of these.

An incident regarding personal data security may occur for a number of reasons, including but not limited to:

- Disclosure of personal data to unauthorized persons;
- Loss or theft of data or devices on which personal data are stored;
- Loss or theft of paper-based records;
- Incorrect access settings that allow unauthorized use of data;
- Violation of Controller's policies on IT security and appropriate use;
- Unauthorized access attempts to computer systems (eg. hackers);
- Erasure or modification of data without permission from the „owner";
- Compromise of IT equipment or networks by viruses or otherwise;
- Physical violations of security, such as the opening of doors, windows by force, opening of containers or compartments containing personal data;
- Disclosure of confidential data in the absence of adequate closure;
- Leaving IT equipment unattended and without a screenlock after login;
- Sending emails containing personal or sensitive data to the wrong recipient.

A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. The GDPR explains that this can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include any other significant economic or social disadvantage to those individuals.

4. Who shall apply this procedure?

This procedure applies to all data users of Controller, including all persons employed by Controller and persons with access to data controlled by Controller for administrative, research or any other purposes.

5. What types of data does this procedure apply to?

This procedure applies to all personal data created or received by Controller in any format (including paper-based data processing), whether it is used in their office, workplace, stored electronically or on a portable device, transported from the workplace physically or electronically or accessed remotely and any other IT systems on which data is held or processed by Controller.

6. Who is responsible in case of personal data breach?

Responsible person in case of incidents violating the security of personal data: Géza Simon, Manager, hereinafter referred to as: Investigator
In emergency situations the control will be taken over by: Géza Simon, Manager

7. Procedure to follow when managing personal data breaches

In line with best practice, the following five steps should be followed in responding to a data security breach:

7.1. **Step 1: Identification and initial assessment**

If Controller or anyone according to Section 4. of this policy considers that a personal data breach has occurred, this must be reported immediately to the Investigator. The Investigator should complete the Personal Data Breach Report Form, Section 1.: Notification **[Annex 5.1., Section 1.]**.

Investigator will determine the severity of the incident using the Checklist **[Annex 5.2.- Checklist for assessing severity of the incident]**. The severity of the incident will be categorized as Level 1, 2 or 3. Following this, Investigator should complete the Personal Data Breach Report Form, Section 2.: Assessment of Severity **[Annex 5.1., Section 2.]** as well.

7.2. **Step 2: Report, communication, immediate remedy, recovery**

Once it has been established that a personal data breach has occurred, or there is a risk of personal data breach, Controller must take immediate and appropriate action to limit or prevent the breach.

If the incident is likely to result in a high risk to the rights and freedoms of the natural person, Investigator is obliged to notify the competent authority, the NAIH, without undue delay, but in any case, within 72 hours from getting aware of the incident. Notification can be made online at: https://dbn-online.naih.hu/public/login by providing the data and information required therein.

Notification is not necessary if Controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Above all, if Company is considered to be the data processor in case of the personal data concerned, Company shall notify the data controller without undue delay.

The Investigator, liaising with the Controller's manager and relevant staff members, will:

- Establish who else other than the data controller, within the Company and the company group needs to be made aware of the breach and inform them of what they are expected to do to abolish the breach (e.g. isolating/closing a compromised section of the network, finding a lost piece of equipment, changing access codes, etc.)
- Establish whether there is anything that can be done to recover any losses and limit the damage caused by the breach (e.g. physical recovery of equipment/records, the use of back-up tapes to restore lost/damaged data).
- Establish if it is reasonable to notify affected individuals immediately (e.g. where there is a high risk to the rights and freedoms of the natural person).

7.3. **Step 3: Risk assessment**

In assessing the risk arising from a personal data breach, Investigator shall consider the potential adverse consequences for those affected, such as the probability of the occurrence of such consequences and how serious or substantial are they likely to be.

In the event of an actual incident, the event has already taken place in terms of risks, therefore the focus is entirely on the risk arising from the impact of the incident on individuals.

The assessment should be based on the examination of the following main criteria:

- Nature of the incident;
- Nature, sensitivity and quantity of personal data;
- Easy identification of individuals;
- The severity of the consequences for individuals;
- Characteristics of the individual;
- Features of Controller;
- Number of individuals affected;
- Other, general aspects.

Investigator will assess the following in connection with the incident:

a) Assess the risks and consequences of the breach:
   Risks for individuals:
   - What are the potential adverse consequences for individuals?
   - How serious or substantial are these consequences?
   - How likely are they to happen?

   Risks for the Controller:
   - Strategic & Operational
   - Compliance/Legal
   - Financial
   - Reputational
   - Continuity of service levels

b) Determine, where appropriate, what further remedial action should be taken on the basis of the incident report to mitigate the impact of the breach and prevent repetition.

Based on the assessment, Investigator shall prepare a report on the personal data breach based on the templates included in the appendix to these Policy as follows:

- a summary of the security breach;
- individuals involved in the breach, (such as staff members, contractors, clients);
- Data (categories and number), IT systems, equipment or devices affected by the incident and data lost or threatened by the incident;
- how the breach occurred;
- actions taken to resolve the breach;

- impact of the data breach;
- unrealised, potential consequences of the data breach;
- Risk classification of the incident
- possible courses of action to prevent further, future data breaches;
- side effects, if any, of those courses of action;
- recommendations for future actions and improvements in data protection as relevant to the incident.

Investigator shall forward the incident report to the Controller's manager, who then will decide on the appropriate measures to be taken.

7.4. **Step 4. Notification of Data Subjects**

Based on the assessment of risks and consequences, Investigator will determine whether it is necessary to notify the breach to others outside the Controller and the NAIH. For example: individuals (data subjects) affected by the breach; other bodies such as other authorities, investors, the press/media; the Controller's insurers, banks, external legal consultants.

In each case, the notification should include at least:

- a description of how and when the breach occurred;
- what data were involved;
- possible consequences;
- what action has been taken to respond to the risks posed by the breach;
- what steps the affected person can take to eliminate the risks;
- name and contact details of the data protection officer or other contact point where more information can be obtained

When notifying individuals, the Investigator should give specific and clear advice on what steps they can take to protect themselves, with which Controller is willing to assist them and should provide details on how to find out further information (e.g. helpline, website).

The Investigator should complete the Personal Data Breach Report Form, Section 3.: Action taken **[Annex 5.1., Section 3.]**.

7.5. Step 5.: Execution

Company shall immediately implement the measures based on the detailed assessment.

7.6. Step 6.: Evaluation and response

Subsequent to a personal data breach, Controller's manager will review the incident in consultation with the relevant responsible persons, to ensure that the steps taken during the incident were appropriate and to identify areas that need further review and improvement.

All personal data breach reports should be sent to Controller's manager who will use these to compile a central record of incidents. Controller will identify conclusions, morals, evidence of possible weaknesses and areas that need to be improved in the future.

7.7. Step 7. Monitoring and communications

Following the assessment of the data breach incident, Controller will carry out monitoring and contacting, communication steps. Possible future monitoring steps can be communication with NAIH, or to keep the data subject informed about the outcome of the personal data breach.

7.8. Step 8: Closure

As the last step of the process, Investigator will close all electronic and paper-based documentation generated during the personal data breach, during which Investigator will seal the relevant Excel chart, provides it with a date and stores it in a password-protected location. Paper-based documents are bound and stored in a place inaccessible to others. Document retention time is, due to the occurrence of possible disputes, 10 years or the time of the final closure of the disputes, according to Infotv.

8. Disclaimer

Controller reserves the right to amend or revoke this Policy at any time without notice and in any manner in which Controller sees fit at the absolute dis-cretion of Controller.

Annex 5.1.

Personal Data Breach Report Form on personal data breach occurred in relation to the data processing of DPC Consulting Kft.

If you discover an event that violates the security of personal data, please complete this form and return it to us at office@dpc.hu as soon as possible.

Section 1. Notification *(To be completed by person discovering/reporting the incident)*

I hereby declare that my personal data provided in this Report Form may be managed by DPC Consulting Kft. based on my freely given consent.		**yes**
		no
Name of person/organisation discovering/reporting the personal data breach:		
Address and other contact details of person/organisation discovering/reporting the personal data breach:		
The start and end date of the incident:		
Date of discovery of the incident:		
The personal data breach is still in progress:		yes
		no
Way of discovering the incident:		
Brief Description of Personal Data Breach:		
Confidentiality:		impaired
		not impaired
Integrity:		impaired
		not impaired
Availability:		impaired
		not impaired

Nature of the incident (multiple responses acceptable)		phishing
		electronic waste (personal data staying on the obsolete device)
		loss or theft of a device
		hacking of IT system
		loss or unauthorized opening of a letter
		losing, stealing, or leaving a paper-based document in a place that is not considered safe
		inappropriate destruction of a paper-based document
		malicious computer programs
		unauthorized access to personal data
		unauthorized verbal communication of personal data

		unauthorized disclosure of personal data to the public
		sending personal data to the wrong recipient
		other
Description of reasons for the personal data breach:		
Number of individuals affected by the incident (if known):		
Group of individuals affected by the incident (e.g. subscribers, employees, etc.):		
Categories of data affected by the incident:		
Consequences of the occurrence of the personal data breach:		
Has any action been taken since the incident occurred?		
Have the affected individuals been informed?		
Is the incident of cross-border nature? If yes, which countries are affected?		
Has the incident been reported to NAIH?		
(This part is to be completed by the recipient of the report)		
Report received by:		
Date:		
Section 2.: Assessment of Severity *(This part is to be completed by Investigator immediately after receiving the report, as a preliminary assessment)*		
IT systems, tools, records involved in the personal data breach:		
Details of the personal data breach:		
What is the nature of the incident?		
What data are affected by the incident?		
Are the data in question unique? Is the nature of the data loss applicable to Controller or to third parties? Is the incident involving operational, research, financial, legal responsibility or reputation?		
How many individuals are affected?		

<table>
<tr><th colspan="2">Annex 5.2.
Checklist for assessing severity of the incident
to to comply with relevant legal obligations</th></tr>
<tr><td colspan="2">Aspects to determine the severity of the incident
- How important is an information tool to the Controller’s business processes or activities?
- Whether the asset is a vital record. Is it unique – once lost, lost forever? Will its loss have adverse financial, liability or reputational consequences e.g. evidential records required to defend the Controller’s interests?
- Is it business-critical? The particular data is accessible through electronic copies or copies on paper e.g. paper files if the data is unavailable from other devices.
- How urgent it is to restore access to information tools or business processes or the restoration of the standard service? Does the personal data breach include sensitive data, that is:
Sensitive data in a case of living, identifiable persons:
- racial or ethnic origin,
- Political opinions, religious or philosophical beliefs,
- trade union membership,
- physical or mental health or condition or sexual life
- commission or alleged commission of any offence, or
- proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.
- Personal information relating to vulnerable adults and children;
- Data that can be used to identify bank account numbers and other financial data and identifiers
- Detailed profiles of individuals; including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;
- Security information that would compromise the safety of individuals if disclosed.</td></tr>
<tr><td rowspan="3">Level 1.:
Local incident</td><td>Meaning: a mild incident in which partial disruption of services or damage to data does not pose a serious threat to the data subject, does not endanger their life, property or environment, or compromise the reputation of Controller</td></tr>
<tr><td>Management: In this case, it is possible to restore the loss or availability of the incident within the framework of normal operation.</td></tr>
<tr><td>Report, notification: In this case the personal data breach is not likely to result in a high risk to the rights and freedoms of natural persons, therefor it is not necessary to report the incident to NAIH or notify the persons affected.</td></tr>
<tr><td rowspan="3">Level 2.:
Severe</td><td>Meaning:
during a severe personal data breach, Controller’s key services are affected by a malfunction, which results in a mild degree of (actual or potential) situation or event threatening life, property or the environment, which is higher than level 1 but lower than level 3, or, if the incident is likely to have significant repercussions on the fundamental rights of the person concerned (cf. high risk personal data breach).</td></tr>
<tr><td>Management: In this case, it is not possible to restore the loss or availability of the incident within the framework of normal operation, special measures are required.</td></tr>
<tr><td>Report, notification: In this case, Controller must evaluate whether the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. If it does, the incident needs to be immediately reported to NAIH and the data subjects affected must be informed.</td></tr>
<tr><td>Level 3.:
Emergency</td><td>Meaning: in the event of an emergency, the termination and restoration of personal data breach or the replacement of the loss of assets or the consequences of their inaccessibility require significant resources of Controller beyond normal operating procedures. In addition, It should also be considered an emergency situation when there is a high number of persons affected or a small number of data subjects affected are subject to extremely serious personal data breach what is unlikely to be fully remediable.</td></tr>
</table>

	Management: Significant special measures are required
	Report, notification: The personal data breach must be immediately reported to NAIH, and all affected data subjects must be informed.

A. Flowchart showing notification requirements