Dealing with personal data breaches

On 25 May 2018, the Swedish Personal Data Act will be replaced by the European Union's General Data Protection Regulation (GDPR).[1] The GDPR introduces an obligation for the controller[2] to notify the Swedish Data Protection Authority if a personal data breach occurs.

The controller is also obliged to inform the data subject[3] of the personal data breach. Processors[4] also have an obligation to report personal data breaches, but to the controller, who is then required to notify the Swedish Data Protection Authority of the breach. The responsibilities of the processor are to be set out in a data processing agreement.

Uppsala University can act as either controller or processor and is therefore responsible for providing notification either to the controller or to the Swedish Data Protection Authority, depending on the situation in the particular case.

Procedures

Uppsala University must have clear and effective procedures to be able to meet the GDPR requirements on notification of personal data breaches. In order to establish whether a personal data breach has taken place and, if necessary, to promptly inform the Swedish Data Protection Authority and the data subject, an account is also required of how appropriate technical and organisational measures have been implemented.

It is highly important to have security solutions in place to avoid breaches. This can be achieved by ensuring that IT systems include functions that notice breaches quickly and that provide a good overview of the types of information that must be reported to the Swedish Data Protection Authority in order to provide notification in time. In addition, data processing agreements must include rules on how to notify Uppsala University of personal data breaches. The current solution gives the IT Division responsibility for compiling and reporting the information required for the data protection officer to assess whether a personal data breach poses a significant risk to the rights and freedoms of natural persons.

Personal data breach

A 'personal data breach' is defined in the GDPR as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.[5] If you become aware of an incident

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[2] The controller is the natural or legal person that, alone or jointly with others, determines the purposes and means of the processing of personal data.

[3] Those whose personal data are processed are called 'data subjects'.

[4] A 'processor' is an actor processing personal data on behalf of another party.

[5] 'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording,

of this kind, it is important that you promptly contact the IT Division at it-incident@uu.se. The IT Division, in turn, will determine whether the Swedish Data Protection Authority is to be notified of the breach.

The notification and its contents

The purpose of the requirement to notify the Swedish Data Protection Authority is to take rapid and appropriate action to reduce the risk of data subjects suffering physical, material or non-material damage. Such damage might involve the loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, damage to reputation or financial loss, for example.[6]

If a personal data breach is detected, Uppsala University must notify the Swedish Data Protection Authority without undue delay and within 72 hours. If it is not possible to provide *all* the information within 72 hours, the information can be divided up and sent in phases as it becomes possible. It is important to give the Swedish Data Protection Authority as much information as possible as promptly as possible.

If the University is unable to provide notification at all within 72 hours, it must inform the Swedish Data Protection Authority, giving reasons for the delay. In cases where the University is the processor, it must notify the controller without undue delay after becoming aware of a personal data breach. The data processing agreement that governs the processing performed by the processor on behalf of the controller sets out the obligations of the processor in the event of a personal data breach in greater detail.

The GDPR states that notification must contain:

- the nature of the breach concerned;
- the categories of persons who may be affected;
- the number of persons affected by the breach;
- the likely consequences of the breach;
- the measures taken to mitigate potential adverse consequences for the data subjects.

Information for those who may be affected

If the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the data subjects must be informed of the breach without undue delay. The purpose of providing this information is to enable the data subject to take precautions.

The question of whether the incident is likely to involve a risk to data subjects and the seriousness of the risk should be assessed on the basis of the nature, scope, context and purpose of the processing. The evaluation of whether the personal data processing involves high risk must be objective. The GDPR defines ‘high risk’ as a particular risk of adverse

---

organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

[6] General Data Protection Regulation, recital 85.

effects for the rights and freedoms of data subjects. This assessment is made by the IT Division after notification to it-incident@uu.se.

When Uppsala University considers that an obligation exists to inform data subjects, this communication must:

- describe in clear and plain language the nature of the personal data breach;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe 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.

However, Uppsala University does not need to inform the data subjects if any of the following circumstances exist:

- The University has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular measures that render the personal data unintelligible to any person who is not authorised to access it, such as encryption.
- The University has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise.
- It would involve disproportionate effort. In such a case, the University must instead issue a public communication or take a similar measure whereby the data subjects are informed in an equally effective manner.

Documentation requirements

Any personal data breaches must be documented, particularly the facts relating to the personal data breach, its effects and the remedial action taken. This documentation is crucial for the University to be able to demonstrate to the Swedish Data Protection Authority that it has taken the measures required to comply with its obligations under the GDPR.

The documentation can serve as input for determining ways of improving security in the University's activities. It can make it possible to verify that necessary measures have been taken to prevent new and similar incidents.

Establishment of procedures

To comply with the provisions of the GDPR, it is important to establish procedures for detecting, reporting and investigating personal data breaches. This involves, in part, appointing one or more persons to deal with personal data breaches and to be responsible for ensuring that they are addressed properly.

The format and procedures for notification of personal data breaches should be determined. When this is done, due consideration should be given to the circumstances of the breach,

including whether or not personal data are protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse.

Notification of personal data breaches

If you suspect or detect a personal data breach, it is important that you communicate this as quickly as possible to it-incident@uu.se so that the IT Division can investigate and if necessary notify the Swedish Data Protection Authority. Mark your email PERSONAL DATA BREACH and give your contact details clearly so that the data protection officer can get in touch with you.