TRAVION
IT DISTRIBUTION

NL

ALGEMENE VERORDENING GEGEVENSBESCHERMING (AVG) DATALEK PROCEDURE

UK

GENERAL DATA PROTECTION REGULATION (GDPR) DATA LEAK PROCEDURE

2018 versie 1.1

Inleiding

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) formeel van kracht. In de AVG is opgenomen dat datalekken verplicht gemeld moeten worden aan de toezichthouder, de Autoriteit Persoonsgegevens, en in bepaalde gevallen ook aan de betrokkene(n) van wie gegevens zijn gelekt.

Er is sprake van een datalek als zich een inbreuk voordoet op beveiligingsmaatregelen, wat leidt tot het per ongeluk, opzettelijk of onrechtmatig vernietigen, verliezen, aanpassen, ongeautoriseerde openbaring van, of toegang tot, persoonsgegevens die overgedragen, bewaard of op een andere manier verwerkt zijn. Voorbeelden van een datalek zijn onder andere:

- Moedwillig handelen: cybercriminaliteit, hacking, identiteitsfraude, malware;
- Technisch falen: fouten in software, storingen;
- Menselijk falen: onzorgvuldige omgang met inloggegevens, nalatigheid;
- Verloren of gestolen apparatuur: laptop, telefoon, externe harddisk, USB stick, server;
- Verzonden e-mail met vertrouwelijke informatie naar meerdere gebruikers met openbaring van e-mailadressen;
- Calamiteit: brand, waterschade.

Een datalek dient uiterlijk **binnen 72 uur** na ontdekking van het datalek te worden gemeld aan de Autoriteit Persoonsgegevens. Indien dit later gebeurt, dient de melding voorzien te worden van uitleg omtrent de vertraging.

Niet ieder datalek-incident valt onder de meldplicht. Artikel 33(1) van de AVG stelt dat een datalek alleen gemeld dient te worden wanneer er een aanzienlijk risico is op schade aan de persoonlijke levenssfeer van een individu. Als bijvoorbeeld verloren of gesloten persoonsgegevens goed versleuteld zijn opgeslagen, dan is er geen aanzienlijke risico op schade aan de persoonlijke levenssfeer.

Procedure datalek

Deze procedure beschrijft de wijze waarop wij omgegaan met de meldplicht datalekken. Het bevat afwegingskaders bij een vermoeden van een datalek en specificeert de nodige acties.

Wij hanteren de volgende stappen in de procedure:

1. Het signaleren, analyseren en registreren van incidenten waarbij er sprake is van een inbreuk op een beveiligingsmaatregel en persoonsgegevens betrokken zijn;
2. Het inhoudelijk beoordelen en onderzoeken van het incident of er op grond van de AVG sprake is van een datalek dat gemeld moet worden;
3. Het melden van het datalek aan de toezichthouder en betrokkenen;
4. Het nemen van maatregelen om het lek te dichten;
5. Het documenteren van het datalek bij zowel interne als externe meldingen.

Melden data incident

De meldplicht datalekken geldt voor de gehele organisatie en voor iedere medewerker. Iedere medewerker die te maken heeft met vermissing/ diefstal van zaken die van Travion zijn of met een informatiebeveiligingsincident, dient dit te melden bij de directie. Dit kan:

- Telefonisch: intern nummer 81
- Per mail: privacy@travion.nl

De medewerker wordt verzocht zijn/ haar naam door te geven met de informatie over het incident. De melder kan namelijk gevraagd worden om aanvullende informatie te geven over het incident. Dit is belangrijk voor de goede en snelle afhandeling van het incident en de volledigheid voor een eventuele melding aan de Autoriteit Persoonsgegevens.

Een extern persoon of organisatie kan op dezelfde manier een data incident of vermoeden van een data incident melden bij Travion.

Registratie data incident

De ontvangen incidentmelding wordt geregistreerd. De volgende gegevens worden vastgelegd:

- Naam van de melder;
- Contactpersoon voor de melding;
- Datum en tijd van de melding;
- Aard van de inbreuk en risico op verlies of onrechtmatig gebruik van gegevens;
- Welke persoonsgegevens vallen onder de melding;
- Om welke gegevensrecords gaat het;
- Welke personen zijn betrokken bij de melding;
- Welke maatregelen zijn getroffen of (kunnen) worden getroffen door de melder;
- Welke gevolgen zijn er volgens de melder voor de betrokkenen.

Beoordelen of er sprake is van een datalek

Zo snel mogelijk na de melding van een incident wordt beoordeelt of er sprake is van een datalek. Zo worden onder andere:

- De gegevens geanalyseerd die zijn vastgelegd bij de registratie van de melding;
- De noodzakelijke vervolgacties vastgesteld met betrekking tot het datalek (lek dichten, toegang tot informatie beperken, meer informatie verzamelen over de indringer);
- Een melding opgesteld voor de Autoriteit Persoonsgegevens (indien melding verplicht);
- De wijze van interne afhandeling bepaald (reactie naar de melder, betrokken medewerkers & afdelingen);
- Uitgezocht of er sprake is van eigen verantwoordelijkheid, aansprakelijkheid van derden of onrechtmatige daad. Afhankelijk hiervan wordt nader bepaald of eventuele schade gedekt is door een verzekeringspolis, of partijen aansprakelijk gesteld moeten worden en/ of aangifte gedaan moet worden bij officiële instanties;
- Bepaald of en welke andere partijen (naast de Autoriteit Persoonsgegevens bijvoorbeeld andere stakeholders, individuen, klanten, prospecten, leveranciers, etc.) geïnformeerd moeten worden.

Als het data incident niet onder een datalek valt, moet het data incident wel in een register worden geregistreerd waarin **alle** data incidenten die zich voordoen in de organisatie geregistreerd worden. Dit betekent dat ook wanneer een lek niet gemeld hoeft te worden, er een documentatieplicht geldt.

Melden aan de Autoriteit Persoonsgegevens

Indien wordt geconstateerd dat er sprake is van een meldenswaardige datalek, moet de datalek binnen 72 uur worden gemeld aan de Autoriteit Persoonsgegevens. Hiervan is sprake als een inbreuk leidt tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van betrokkenen. Hierbij spelen de volgende factoren een rol:

1. Zijn er persoonsgegevens van gevoelige aard gelekt?
   Het betreft hier een incident waarbij bijzondere persoonsgegevens, zoals medische gegevens, politiegegevens, gegevens over ras of religie of financiële gegevens zijn gelekt;
2. Leiden de aard en omvang van de inbreuk tot een aanzienlijk risico op schade aan de persoonlijke levenssfeer van een individu?
   Naarmate meer gevoelige gegevens in het geding zijn (ofwel van meerdere personen ofwel veel gegevens van een persoon) zal er eerder sprake zijn van een datalek dat moet worden gemeld.

Er moet in ieder geval gemeld worden als één van onderstaande vragen positief wordt beantwoord.

Vraag	Antwoord	Actie
Zijn gegevens (definitief) verloren gegaan?	JA	Melden
Zijn de gegevens bijzonder of zeer omvangrijk?	JA	Melden
Zijn de gegevens in onbevoegde handen geraakt?	JA	Melden
Aanzienlijk risico op schade aan persoonlijke levenssfeer?	JA	Melden
NEE op alle vragen ➔ **NIET MELDEN**		

Bij een melding aan de Autoriteit Persoonsgegevens wordt onder andere doorgegeven:

- Aard van de inbreuk: betrokken categorieën, aantal betrokkenen, beschrijving van gegevens;
- Beschrijving van de (te verwachten) gevolgen;
- De maatregelen die zijn genomen en/ of worden genomen om de schade voor betrokkene(n) te verkleinen;
- De maatregelen die betrokkene(n) kunnen nemen om verdere schade te verkleinen;
- Contactgegevens voor betrokkene(n).

Melden aan betrokkene(n)?

De betrokkene is degene over wie persoonsgegevens worden verwerkt en waarvan de gegevens onderwerp zijn van de datalek. Indien er sprake is van een datalek, moet deze aan de betrokkene worden gemeld, als de inbreuk een hoog risico brengt op schade aan diens persoonlijke levenssfeer. Niet in alle gevallen hoeft een datalek aan de betrokkene te worden gemeld. Voor de beoordeling of aan de betrokkene(n) gemeld moet worden, zijn de volgende vragen van belang:

Vraag	Antwoord	Actie
Zijn er zwaarwegende redenen om de melding aan de betrokkene achterwege te laten?	NEE	Melden
Zijn de gegevens versleuteld of ontoegankelijk voor degene die geen recht op inzage heeft in deze gegevens	NEE	Melden

Artikel 34(3) van de AVG stelt drie voorwaarden waaronder geen melding aan betrokkenen vereist is. Dit geldt in de volgende situaties:

1. Er zijn technische en organisatorische maatregelen getroffen ter bescherming van de persoonsgegevens *vooraf* aan het lek. In het bijzonder maatregelen die ervoor zorgen dat de data niet toegankelijk is voor ongeautoriseerde personen. Bijvoorbeeld door encryptie of anonimiseren;
2. Direct na een datalek zijn er acties ondernomen om ervoor te zorgen dat er geen hoog risico meer is op schade aan de persoonlijke levenssfeer van betrokkenen;
3. Het zou van onevenredige moeite zijn om contact op te nemen met individuen, bijvoorbeeld wanneer de contactgegevens van betrokkenen verloren zijn. In dit geval zal er gekozen moeten worden voor een openbare communicatie uiting of een vergelijkbare maatregel.

Termijn van melden

Voor het melden van een datalek aan betrokkenen geldt dat dit 'onverwijld' moet gebeuren. Uitgangspunt is dat onnodige vertraging wordt voorkomen, zodat de betrokkene de nodige maatregelen kan treffen. Een datalek dient echter altijd binnen 72 uur te worden gemeld aan de toezichthouder!

Melden aan andere partijen?

Indien sprake is van samenwerking met andere partijen (ketenverwerking of verwerkers) zullen wij beoordelen of een datalek-incident aan de externe partij gemeld moet worden. Dit is geen wettelijke verplichting, maar kan vanuit communicatie redenen raadzaam zijn.

Afhandelen van een melding

Elke melding wordt geregistreerd in het register van datalekken. In dit register worden zowel de intern als de externe meldingen geregistreerd.

Travion IT Distribution B.V.
Postbus 154
6500 AD Nijmegen
Telefoon: +31 (0)24 – 357 88 22
E-mail: info@travion.nl
KvK-nummer: 09120764

Introduction

As of May 25, 2018, the General Data Protection Regulation (GDPR) will formally come into force. The GDPR states that data leaks must be reported to the supervisory authority, the Dutch Data Protection Authority, and in certain cases also to the data subject(s) whose data has been leaked.

A data breach occurs when there is a breach of security measures, resulting in the accidental, intentional or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data that has been transferred, stored or otherwise processed . Examples of a data breach include:
• Willful act: cybercrime, hacking, identity fraud, malware;
• Technical failure: errors in software, malfunctions;
• Human failure: careless handling of login data, negligence;
• Lost or stolen equipment: laptop, telephone, external hard disk, USB stick, server;
• Sent e-mail containing confidential information to multiple users with disclosure of e-mail addresses;
• Calamity: fire, water damage.

A data breach must be reported to the **within 72 hours** of discovery of the data breach
Authority for Personal Data. If this happens later, the notification must be accompanied by an explanation of the delay.

Not every data breach incident falls under the reporting obligation. Article 33(1) of the GDPR states that a data breach should only be reported when there is a significant risk of damage to the privacy of an individual. For example, if lost or closed personal data is stored properly encrypted, there is no significant risk of damage to privacy.

Data breach procedure

This procedure describes the way in which we deal with the data breach notification obligation. It contains assessment frameworks in the event of a suspected data breach and specifies the necessary actions.

We use the following steps in the procedure:
1. Identifying, analyzing and registering incidents involving a breach of a security measure and involving personal data;
2. Assessing and investigating the content of the incident whether there is a data breach that must be reported on the basis of the AVG;
3. Reporting the data breach to the supervisor and those involved;
4. Taking measures to close the leak;
5. Documenting the data breach in both internal and external reports.

Report data incident

The obligation to report data breaches applies to the entire organization and to every employee. Every employee who is involved in the loss/theft of items belonging to Travion or with an information security incident must report this to the management. This is possible:
• By phone: internal number 81
• By email: privacy@travion.nl

The employee is requested to provide his/her name with the information about the incident. The reporter may be asked to provide additional information about the incident. This is important for the proper and rapid handling of the incident and the completeness of a possible report to the Dutch Data Protection Authority.

An external person or organization can report a data incident or suspected data incident to Travion in the same way.

Registration data incident

The received incident report is registered. The following data is recorded:
• Name of the reporter;
• Contact person for the report;
• Date and time of the notification;
• Nature of the breach and risk of loss or unlawful use of data;
• Which personal data are covered by the report;
• Which data records are involved;
• Which persons are involved in the report;
• Which measures have been taken or (can be) taken by the reporter;
• What are the consequences for those involved according to the reporter?

Assess whether there is a data breach

As soon as possible after an incident has been reported, an assessment is made to determine whether there has been a data breach. For example:
• Analyzed the data recorded when registering the report;
• Determined the necessary follow-up actions with regard to the data breach (fix the leak, restrict access to information, collect more information about the intruder);
• A notification drawn up for the Dutch Data Protection Authority (if notification is required);
• Determine the internal handling method (response to the reporter, employees & departments involved);
• Determined whether there is personal responsibility, liability of third parties or tort. Depending on this, it will be determined in more detail whether any damage is covered by an insurance policy, whether the parties must be held liable and/or whether a declaration must be made to official authorities;
• Determine whether and which other parties (besides the Dutch Data Protection Authority, for example, other stakeholders, individuals, customers, prospects, suppliers, etc.) must be informed.

If the data incident does not fall under a data breach, the data incident must be registered in a register in which all data incidents that occur in the organization are registered. This means that even if a leak does not have to be reported, there is a documentation obligation.

Report to the Dutch Data Protection Authority

If it is established that there is a reportable data breach, the data breach must be reported to the Dutch Data Protection Authority within 72 hours. This is the case if an infringement leads to a significant risk of damage to the privacy of those involved. The following factors play a role here:
1. Has personal data of a sensitive nature been leaked?
This concerns an incident in which special personal data, such as medical data, police data, data about race or religion or financial data have been leaked;
2. Does the nature and extent of the infringement lead to a significant risk of damage to an individual's privacy?
The more sensitive data is at stake (either from several people or a lot of data from one person), the more likely there will be a data breach that must be reported.

In any case, you must report if one of the questions below is answered positive.

Vraag	Antwoord	Actie
Has data been (permanently) lost?	JA	Melden
Is the data special or very extensive?	JA	Melden
Did the data fall into unauthorized hands?	JA	Melden
Significant risk of damage to privacy?	JA	Melden
NO to all questions ➔ **DO NOT REPORT**		

When reporting to the Dutch Data Protection Authority, among other things:
• Nature of the infringement: categories involved, number of data subjects, description of data;
• Description of the (expected) consequences;
• The measures that have been taken and/or are being taken to reduce the damage for the person(s) involved;
• The measures that the person(s) involved can take to reduce further damage;
• Contact details for the person(s) involved.

Report to the person(s) involved?

The data subject is the person about whom personal data is processed and whose data is the subject of the data breach. If there is a data breach, it must be reported to the data subject, if the breach poses a high risk of damage to their privacy. A data breach does not have to be reported to the data subject in all cases. The following questions are important for the assessment of whether the data subject(s) must be notified:

Question	Answer	Action
Are there compelling reasons not to notify the data subject?	No	Report
Are the data encrypted or inaccessible to those who do not have the right to inspect this data?	No	Report

Article 34(3) of the GDPR sets three conditions under which no notification to data subjects is required. This applies in the following situations:
1. Technical and organizational measures have been taken to protect the personal data prior to the leak. In particular, measures that ensure that the data is not accessible to unauthorized persons. For example by encryption or anonymization;
2. Immediately after a data breach, actions are taken to ensure that there is no longer a high risk of damage to the privacy of those involved;
3. It would be disproportionate to contact individuals, for example where contact details of data subjects are lost. In this case, a public communication or a comparable measure will have to be chosen.

Term of reporting

Reporting a data breach to data subjects must be done 'immediately'. The basic principle is that unnecessary delays are prevented, so that the person concerned can take the necessary measures. However, a data breach must always be reported to the supervisor within 72 hours!

Report to other parties?

If there is cooperation with other parties (chain processing or processors), we will assess whether a data breach incident must be reported to the external party. This is not a legal obligation, but may be advisable for communication reasons.

Handling a report

Every report is registered in the register of data breaches. Both internal and external reports are registered in this register.

Travion B.V.
PO Box 154
6500 AD Nijmegen
Phone: +31 (0)24 – 357 88 22
Email: info@travion.nl
Chamber of Commerce number: 09120764