Protocol melding van datalekken en het verstrekken van informatie van Stichting Surplus

1. Inleiding

Een datalek is een beveiligingsincident waarbij persoonsgegevens, die de ene medeverantwoordelijke namens de andere medeverantwoordelijke beheert, mogelijk verloren zijn gegaan of onbedoeld toegankelijk waren voor derden. Elke medeverantwoordelijke dient voor het deel waar hij/zij verantwoordelijk voor is een melding te maken bij de toezichthoudende autoriteit wanneer er sprake is van een beveiligingsincident. Het gaat om gegevens die te koppelen zijn aan personen, zoals, maar niet beperkt tot, namen, adressen, telefoonnummers, e-mailadressen, login-gegevens, cookies, IP-adressen of identificerende gegevens van computers of telefoons.

Hieronder vind je een aantal voorbeelden van beveiligingsincidenten die moeten worden gemeld bij de Autoriteit Persoonsgegevens:

- De website met login-gegeven is gehackt of is toegankelijk voor derden.
- Verlies van laptop of USB-stick met persoonsgegevens.
- Salarisstroken van medewerkers zijn per ongeluk naar verkeerde personen gestuurd.
- Brieven of e-mails worden naar een verkeerd adres gestuurd.
- Een aanval van een hacker op het ICT-systeem.
- Een verloren of gestolen telefoon waar persoonsgegevens op aanwezig zijn.

2. Wat te doen bij twijfel?

Als je op basis van bovenstaande niet zeker weet of er sprake is van een beveiligingsincident, stel voor jezelf in ieder geval alvast de volgende vragen als hulpmiddel:

- Zijn er technische of fysieke beveiligingsproblemen?
- Gaat het probleem over de beveiliging van persoonsgegevens? Ook IP-adressen telefoonnummers of identificerende gegevens, bijvoorbeeld van hardware zoals een IMEI-nummer, kunnen hieronder vallen.
- Gaat het om gevoelige gegevens zoals ras, gezondheidsgegevens , informatie over iemands financiële situatie, zoals salaris of gegevens waar (identiteits-)fraude mee kan worden gepleegd, zoals een BSN nummer?
- Zijn er grote hoeveelheden persoonsgegevens onbedoeld toegankelijk geworden voor derden?
- Gaat het om gegevens van kwetsbare groepen zoals kinderen?
- Worden de persoonsgegevens beheerd door een leverancier?

Ook wanneer je twijfelt, neem het zekere voor het onzekere en neem altijd contact op met:

Medeverantwoordelijke 1:
Jack ten Haaf
Directeur/ Bestuurder

Medeverantwoordelijke 2:
Richard Bosma
Kwaliteitsmedewerker

3. Waar meld je het beveiligingsincident?

Als je een beveiligingsincident hebt ontdekt, neem je direct contact op met:

Medeverantwoordelijke 1:
Jack ten Haaf
Directeur/ Bestuurder
Telefoon: 053 206 8200
E-mail: tenhaaf@st-surplus.nl

Medeverantwoordelijke 2:
Richard Bosma
Kwaliteitsmedewerker
Telefoon: 053 206 8200
E-mail: r.bosma@st-surplus.nl

4. Geef in je e-mail antwoord op de onderstaande vragen

De onderstaande vragen zijn gelijk aan de informatie die aan de Autoriteit Persoonsgegevens moet worden verstrekt wanneer van het datalek een melding gemaakt moet worden.

Richard Bosma kan je helpen met de beantwoording hiervan. Gaarne de vragen zo volledig mogelijk en schriftelijk beantwoorden.

1. Geef een samenvatting van het beveiligingslek/ beveiligingsincident/ datalek: wat is er gebeurd? Vermeld hier ook de naam van het betrokken systeem.
2. Welke typen Persoonsgegevens zijn betrokken bij het beveiligingsincident?
   Zoals, maar niet beperkt tot, naam, adres, e-mailadres, IP-nummer, Burgerservicenummer, pasfoto en ieder ander tot een persoon te herleiden gegeven.
3. Van hoeveel personen zijn de Persoonsgegevens betrokken bij het beveiligingsincident? Geef a.u.b. een minimum en een maximum aantal personen.
4. Omschrijving groep personen om wiens gegevens het gaat. Geef aan of het gaat om medewerkersgegevens, gegevens van internetgebruikers. Bijzondere aandacht verdienen gegevens van kwetsbare groepen personen, zoals kinderen.
5. Zijn de contactgegevens van de betrokken personen bekend?
   Het kan zijn dat de betrokkenen geïnformeerd moeten worden over het datalek, kunnen we deze personen in dat geval bereiken?
6. Wat is de oorzaak (root cause) van het beveiligingsincident?
   Heeft u een idee hoe het beveiligingsincident heeft kunnen ontstaan?
7. Op welke datum of in welke periode heeft het incident plaats kunnen vinden?
   Geef a.u.b. zo specifiek mogelijk aan.