Stappenplan melden datalekken

Wat te doen bij een (vermeend) datalek?

Versie	Datum	Opmerkingen
1.0	26-6-2018	Vastgesteld CvB

INLEIDING

Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. En soms moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). Daartoe heeft ROC TOP een stappenplan gebouwd.

WAT IS EEN DATALEK?

Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens.

We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens[1] (art. 33 en 34 AVG). Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.

Voorbeelden van datalekken zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker.

WAT ZIJN PERSOONSGEGEVENS?

De Algemene Verordening Gegevensbescherming (AVG) geeft aan dat een persoonsgegeven elk gegeven is over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Dat het om een natuurlijke persoon moet gaan, houdt in dat gegevens van overleden personen of van organisaties geen persoonsgegevens zijn. Er zijn vele soorten persoonsgegevens. Voor de hand liggende gegevens zijn iemands naam, adres en woonplaats. Maar ook telefoonnummers en postcodes met huisnummers zijn persoonsgegevens. Gevoelige gegevens als iemands ras, godsdienst of gezondheid worden ook wel bijzondere persoonsgegevens genoemd. Deze zijn door de wetgever extra beschermd.

De AVG stelt strenge eisen aan de eigen registratie van de datalekken die zich in uw organisatie hebben voorgedaan. Alle datalekken moeten worden gedocumenteerd. Met deze documentatie moet de AP kunnen controleren of aan de meldplicht wordt voldaan.

[1] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/beveiliging-van-persoonsgegevens

STAPPENPLAN

Bij ROC TOP volgen we de volgende stappen als we met een mogelijk datalek te maken hebben. Iedereen binnen ROC TOP kan een datalek ontdekken en melden.

1. De ontdekker van het datalek meldt het:
   a. Bij zijn/haar leidinggevende of teamleider (ook in geval van studenten), of
   b. Bij de Functionaris voor de Gegevensbescherming (FG).
   c. De leidinggevende geeft het lek door aan de FG.

2. De FG beoordeelt of het om een datalek gaat. Er zijn twee uitkomsten mogelijk:
   a. Het is geen datalek. Het reguliere incidentenproces is van toepassing.
   b. Het is een datalek. Melding bij de Autoriteit Persoonsgegevens en eventuele betrokkenen is noodzakelijk.
3. In geval van een datalek roept de FG de leden van het IBP-overleg, eventueel aangevuld met andere relevante functionarissen, zo snel als mogelijk bijeen om tot een oplossing te komen.

4. Een datalek wordt gemeld bij de Autoriteit Persoonsgegevens door de persoon die daartoe bevoegd is (de Functionaris Gegevensbescherming), binnen 72 uur na ontdekking.

5. Indien noodzakelijk bericht het IBP-overleg de betrokkenen.

6. Na eventuele melding bij de AP stelt het IBP-overleg een onderzoek in naar de toedracht van het incident en maakt daar een rapportage van op. In die rapportage worden de volgende zaken opgenomen:
   a. De originele melding en melder.
   b. De genomen stappen tijdens het onderzoek.
   c. Een uiteenzetting van de bestudeerde documentatie.
   d. De gekozen verbetermaatregel(en).
   e. Of, als het om een datalek ging, de betrokkene(n) wel of niet worden ingelicht over hun gelekte gegevens. Dit is vaak bij stap 2 al duidelijk, omdat die vraag ook door de AP gesteld wordt bij het doen van een melding (stap 4).

7. Het rapport wordt minimaal 1 jaar bewaard.

Contactgegevens

Functionaris voor de gegevensbescherming ROC TOP	Functionaris Gegevensbescherming NDSM straat 1 1033 SB Amsterdam fg@roctop.nl
De Autoriteit Persoonsgegevens	Postbus 93374 2509 AJ Den Haag

Voorbeelden van een datalek

Soort data lek	Toelichting
Een wachtwoord is bekend bij anderen dan de eigenaar.	Hierdoor is onbevoegde toegang tot- en misbruik van- informatie mogelijk.
Privacygevoelige informatie van het ROCTOP(brief, mail, factuur) is beland bij iemand anders dan de geadresseerde.	1) ROCTOP ontvangt een melding (telefonisch, per mail of per brief) dat post van het ROCTOP op een verkeerd adres is bezorgd. Leg in ieder geval vast: welke persoon het betreft en wat zijn gegevens van degene die de melding doet. 2) Je ontdekt dat je per ongeluk een mail met privacygevoelige informatie aan de verkeerde persoon hebt verzonden. Nb: privacygevoelige informatie mag niet onbeveiligd per mail verzonden worden.
Fout met autorisaties.	1) Je hebt meer rechten om informatie in te zien en te bewerken dan je voor je werk nodig hebt. 2) Je hebt een andere functie/taak gekregen. Naast je nieuwe autorisaties heb je ten onrechte nog steeds je oude autorisaties. 3) Een collega is uit dienst. Je constateert dat hij nog steeds een actief account heeft (je merkt dit bijv. als je een mailtje stuurt naar en collega die al langer dan een week uit dienst is en je krijgt geen foutmelding op de mail).
N.a.v. een informatieverzoek van ketenpartners om privacygevoelige informatie wordt deze informatie ten onrechte uitgeleverd.	Commerciële partijen en/of gemeenten vragen selecties op van studenten en/of medewerker gegevens. Om deze te mogen leveren moet er een formele afspraak met goedkeuring van de gegevenseigenaar aanwezig zijn. Indien dit niet het geval is dient altijd eerst de FG geraadpleegd te worden.
Onbevoegde toegang	Hier behoren o.a. toe: -Toegang tot databases met privacy gevoelige gegevens door onbevoegde personen; -Een externe hacker krijgt toegang tot privacygevoelige informatie.
Gebruik van productiegegevens in test/ontwikkelomgevingen	Er mag niet worden getest / ontwikkeld met gebruik van productiegegevens. Als dit niet anders kan dient expliciete toestemming van de data eigenaar aanwezig te zijn (mail of schriftelijk).
Systeemfouten	Persoonsinformatie is zichtbaar buiten het daarvoor ingerichte systeem
Logistiek	Post / mail / bestand is op verkeerde adres bezorgd en de ontvanger heeft deze geopend.