Protocol Datalekken

Het Protocol vormt een handleiding voor de interne melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken.

www.vcsw.nl

VCSW B.V.
Postbus 90422
2509 LK Den Haag

PROTOCOL DATALEKKEN VCSW – juli 2020

1. Inleiding

Dit Protocol Datalekken (hierna: het Protocol) is gebaseerd op het informatiebeveiligings- en privacy-beleid van de besloten vennootschap VCSW B.V. (hierna: de Organisatie).

Het Protocol vormt een handleiding voor de interne melding, beoordeling en afhandeling van beveiligings-incidenten en datalekken. Het doel ervan is het in voorkomend geval adequaat, nodig en tijdig melden van datalekken aan de Autoriteit Persoonsgegevens en indien van toepassing aan de betrokkene(n). Daarnaast beoogt het Protocol het voorkomen van beveiligingsincidenten en datalekken.

Het Protocol is van toepassing op de gehele organisatie van de Organisatie en al haar medewerkers.

Gebruikte begrippen:

Beveiligingsincident:	een gebeurtenis die er voor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de systemen van de Organisatie wordt aangetast.
Datalek:	een inbreuk in verband met persoonsgegevens, zijnde een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens. Alle datalekken zijn beveiligingsincidenten; niet alle beveiligingsincidenten zijn datalekken: namelijk incidenten waarbij geen persoonsgegevens zijn betrokken zijn geen datalekken. Voorbeelden van beveiligingsincidenten die ook een datalek kunnen zijn: e-mail aan verkeerde geadresseerde sturen, verlies of diefstal USB-stick/laptop, een hack, ransomware-besmetting, weggooien niet behoorlijk vernietigd papier of verkeerde klantgegevens in portal tonen.
Betrokkene:	de persoon wiens persoonsgegevens zijn gelekt.

2. Wet- en regelgeving datalekken

2.1. De meldplicht datalekken is gebaseerd op de artikelen 33 en 34 AVG. Op grond daarvan is een verwerkingsverantwoordelijke verplicht zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, een datalek te melden aan de Autoriteit Persoonsgegevens.

Er is geen meldplicht als het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Echter het nalaten van het doen van een verplichte melding kan leiden tot een hoge boete.

2.2. Ook is de verwerkingsverantwoordelijke verplicht de betrokkene het datalek onverwijld mee te delen, als het datalek een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

2.3. Kort gezegd, als er naw-gegevens en een e-mail adres worden gelekt, zal een risico voor de rechten en vrijheden niet snel te vrezen zijn. Als die gegevens gekoppeld zijn aan bijzondere persoonsgegevens, zoals medische gegevens, seksuele of politieke voorkeur of als er financiële gegevens of BSN zijn gelekt, dan is dat risico er wel. Zijn de gegevens echter op een goede manier encrypted dan is dit risico er (mogelijk) niet.

Meer specifiek en volledig: Er is sprake van een risico voor de rechten en vrijheden van natuurlijke personen als het datalek kan resulteren in ernstige lichamelijke, materiële of immateriële schade, met name: waar de verwerking kan leiden tot discriminatie, identiteitsdiefstal of -fraude, financiële verliezen, reputatieschade, verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens, ongeoorloofde ongedaanmaking van pseudonimisering, of enig ander aanzienlijk economisch of maatschappelijk nadeel.

En voorts als de betrokkenen hun rechten en vrijheden niet kunnen uitoefenen of worden verhinderd controle over hun persoonsgegevens uit te oefenen; als persoonsgegevens worden verwerkt waaruit ras of etnische afkomst, politieke opvattingen, religie of levensbeschouwelijke overtuigingen, of vakbondslidmaatschap blijkt, en bij de verwerking van genetische gegevens of gegevens over gezondheid of seksueel gedrag of strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen; als persoonlijke aspecten worden geëvalueerd, om met name beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen te analyseren of te voorspellen, teneinde persoonlijke profielen op te stellen of te gebruiken; als persoonsgegevens van kwetsbare natuurlijke personen, met name van kinderen, worden verwerkt; of als de verwerking een grote hoeveelheid persoonsgegevens betreft en gevolgen heeft voor een groot aantal betrokkenen.

2.4. Als de organisatie geen verwerkingsverantwoordelijke is maar verwerker, dan moet de verwerker zonder onredelijke vertraging het datalek melden aan de verwerkingsverantwoordelijke.

2.5. Indien een (sub)verwerker een beveiligingsincident meldt, dan treedt dit Protocol eveneens in werking.

3. Procedure actieplan datalek

3.1. Alle beveiligingsincidenten moeten onmiddellijk intern per e-mail en in vermoedelijk ernstige gevallen mondeling worden gemeld aan de Bedrijfs- en Kwaliteitsanalist of in geval van afwezigheid bij zijn vervanger. Bij een vermoedelijk ernstig datalek wordt de (vervangende) Bedrijfs- en Kwaliteitsanalist ook onmiddellijk mondeling geïnformeerd. De interne melding kan door iedere medewerker worden gedaan.

3.2. Wordt de melding door een derde gedaan aan de Organisatie, dan wordt te allen tijde eerst van de melder zijn contactgegevens vastgelegd, zodat het mogelijk is bij de melder nadere informatie op te vragen. Daarnaast worden zoveel mogelijk relevante gegevens over het gemelde incident genoteerd.

3.3. Alle medewerkers van de Organisatie moeten van 3.1 en 3.2 op de hoogte zijn.

3.4. De Bedrijfs- en Kwaliteitsanalist documenteert terstond het datalek en legt onmiddellijk de volgende informatie over het datalek vast:

a. naam melder en datum en tijdstip melding;
b. de aard van het beveiligingsincident,
c. indien beschikbaar en van toepassing alle logfiles i.v.m. het datalek,
d. de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie,
e. of de Organisatie terzake het beveiligingsincident verwerker of verwerkingsverantwoordelijke is,
f. de waarschijnlijke gevolgen van de inbreuk,
g. overige relevante gegevens.
h. Voorts inventariseert hij de maatregelen die genomen kunnen worden om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen.

3.5. De Bedrijfs- en Kwaliteitsanalist informeert aansluitend de Functionaris voor Gegevensbescherming en overlegt met hem.

3.6. Eerste analyse

De Bedrijfs- en Kwaliteitsanalist én de Functionaris Gegevensbescherming overleggen of het beveiligingsincident vermoedelijk een meldplichtig datalek is.

De volgende beslisboom kan worden gehanteerd:

3.7. Het overleg kan leiden tot de volgende conclusies:

a. Er is geen sprake van een meldplichtig datalek;
b. Er is vermoedelijk geen sprake van een meldplichtig datalek;
c. Er is vermoedelijk wél sprake van een meldplichtig datalek;

Ad a. Er is geen sprake van een meldplichtig datalek

In dat geval worden de volgende maatregelen genomen:

- registratie van de melding door de Bedrijfs- en Kwaliteitsanalist;
- inventariseren en treffen van maatregelen om herhaling te voorkomen;
- interne mededeling aan de direct betrokkenen w.o. de melder over de afhandeling;
- de melding wordt afgesloten.

Ad b. Er is vermoedelijk geen sprake van een meldplichtig datalek

De verzamelende informatie over het datalek met de voorlopige conclusie wordt per e-mail voorgelegd aan het Responseteam (zie hierna). Elk lid beoordeelt direct of het datalek al dan niet als meldplichtig moet worden aangemerkt (de eerder genoemde beslisboom kan worden gebruikt) en bericht de Bedrijfs- en Kwaliteitsanalist over de bevinding.

Als alle leden menen dat er geen sprake is van een meldplichtig datalek dan volgt de procedure onder ad a. Meent een lid dat er wel sprake is van een meldplichtig datalek dan volgt de procedure onder ad c.

Ad c. Er is vermoedelijk wél sprake van een meldplichtig datalek
Is er vermoedelijk wel sprake van een meldplichtig datalek, dan roept de Bedrijfs- en Kwaliteitsanalist direct het Responseteam bijeen.

4. Het Responseteam

4.1. Het Responseteam, bestaande uit:

- Directeur van de Organisatie of zijn vervanger;
- Functionaris voor Gegevensbescherming
- Bedrijfs- en Kwaliteitsanalist
- IT-beheerder, indien het lek IT-gerelateerd is of kan zijn
- Verantwoordelijk manager afdeling waar het lek zich heeft voorgedaan.

4.2. Het Responseteam overlegt en beslist over:

1. of de Organisatie terzake het datalek verwerker is of verwerkingsverantwoordelijke. In het 1e geval meldt de Organisatie uitsluitend aan de verwerkingsverantwoordelijke en nimmer aan de AP of betrokkenen omdat dit de uitsluitende verantwoordelijkheid is van de verwerkingsverantwoordelijke;
2. als de Organisatie verwerker is, geldt het onderstaande onverminderd, met dien verstande dat voor “AP” en “betrokkene”; “verwerkingsverantwoordelijke” gelezen moet worden;
3. of het datalek bij de AP gemeld moet worden en zo ja wat er gemeld moet worden;
4. zo ja, dan draagt de Bedrijfs- en Kwaliteitsanalist zorg voor tijdige melding;
5. of het datalek bij de betrokkene(n) gemeld moet worden en welke mededeling gedaan moet worden;
6. zo ja, dan draagt de Bedrijfs- en Kwaliteitsanalist zorg voor onverwijlde mededeling;
7. de geïnventariseerde maatregelen om de inbreuk aan te pakken en toegang tot informatie (tijdelijk) te beperken;
8. de te treffen maatregelen om herhaling te voorkomen;
9. de te treffen maatregelen om de nadelige gevolgen en/of schade voor betrokkenen te vermijden of te beperken;
10. overige relevantie maatregelen, zoals de wens en noodzakelijkheid van crisiscommunicatie en/of communicatie met de pers;

11. de wijze van afhandeling intern, inclusief communicatie naar melder, betreffende afdeling(-en) en manager(s);
12. het al dan niet melden van het datalek bij de relevante verzekeraars;
13. het al dan doen van aangifte van strafbare feiten
14. het al dan niet inwinnen van juridisch advies over een of meer van de bovenstaande onderwerpen.
15. hetgeen intern gecommuniceerd wordt, op welk moment;
16. hetgeen extern gecommuniceerd wordt, op welk moment;
17. of er ook andere stakeholders geïnformeerd worden.

Indien het datalek zich voordoet en ontdekt wordt buiten kantoortijden, dan handelt de Bedrijfs- en Kwaliteitsanalist of zijn vervanger naar bevindt van zaken, waarbij de ernst en omvang van het datalek worden meegewogen, en tracht hij zoveel mogelijk leden van het responseteam te bereiken en te betrekken. De Organisatie heeft maatregelen genomen om ervoor te zorgen dat het Responseteam en/of de vervangende leden ervan redelijk tot goed bereikbaar zijn.

Dit protocol kan van tijd tot tijd worden aangepast.