TT3P Template Protocol Datalekken

De wet Algemene Verordening Persoonsgegevens (AVG) bepaalt dat datalekken direct, binnen 72 uur, gemeld moeten worden aan de Autoriteit Persoonsgegevens (AP), tenzij het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen.
Daarnaast moet het datalek ook aan de betrokkenen gemeld worden indien het waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen met zich meebrengt.
Aan de beantwoording van de vraag moet een zorgvuldige (belangen)afweging voorafgaan. Hierbij is bijvoorbeeld de aard en de omvang van de persoonsgegevens die gelekt zijn van belang. Als er bijzondere persoonsgegevens, zoals gegevens over gezondheid, gelekt zijn, dan is de melding meestal noodzakelijk. Dit Template Protocol Datalekken is bedoeld als hulpmiddel voor de beantwoording van de vraag of er sprake is van een datalek en of deze gemeld moet worden.

SCOPE

Er is sprake van een datalek als er een inbreuk in verband met persoonsgegevens heeft plaatsgevonden. Alleen een dreiging of een tekortkoming in de beveiliging is niet voldoende; er moeten daadwerkelijk persoonsgegevens gelekt zijn.

Onder een datalek verstaat de AP persoonsgegevens die gelekt of vernietigd zijn als gevolg van een beveiligingsincident. Bij het lek zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking. Bij verlies zijn de persoonsgegevens er niet meer. Onder onrechtmatige verwerking vallen bijvoorbeeld onbevoegde kennisneming, wijziging, aantasting of de verstrekking daarvan.

Voorbeelden van inbreuken in verband met persoonsgegevens kunnen zijn:

- kwijtraken van een USB -stick;
- diefstal van een laptop;
- inbraak door een hacker;
- per ongeluk gepubliceerde persoonsgegevens;
- hacking, mailware of phishing;
- persoonsgegevens aan verkeerde persoon verstuurd.

VOORBEELD BELEID

CONTACTPERSOON DATALEKKEN

[BEDRIJFSNAAM] heeft een eigen Contactpersoon Datalekken aangewezen aan wie eventuele datalekken gemeld moeten worden.

INFORMEREN MEDEWERKERS

Medewerkers binnen [BEDRIJFSNAAM] zijn zich ervan bewust dat als er sprake is van een datalek, zij dit datalek direct (diezelfde dag nog) moeten melden bij de aangewezen Contactpersoon Datalekken, zodat deze tijdig het datalek kan melden bij de Autoriteit Persoonsgegevens.

UITVOEREN VAN HET STAPPENPLAN DATALEKKEN

De binnen [BEDRIJFSNAAM] aangewezen Contactpersoon Datalekken draagt zorg voor de invoering en naleving van het hieronder opgenomen stappenplan Datalekken. Indien er een datalek optreedt dienen de Stappen in het stappenplan Datalekken doorlopen te worden.

STAPPENPLAN DATALEKKEN

Processtappen	Activiteit	Verantwoordelijke persoon
1. Er wordt een (mogelijk) datalek ontdekt	• Maak direct intern melding van (mogelijke) datalek • Informeer de verantwoordelijke Contactpersoon Datalekken	Medewerker die het ontdekt
2. Beoordeel het datalek	• Onderzoek het beveiligingsincident • Onderzoek of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden • Beoordeel wie of welke afdelingen binnen de organisatie hierbij betrokken zijn • Beoordeel of er een verwerker betrokken is bij het incident. Zo ja dan dient deze bij het proces betrokken te worden	Contactpersoon Datalekken
3. Bestrijdt het datalek	• Stop het datalek als het nog kan • Neem andere maatregelen om het datalek en de daaruit voortvloeiende schade te beperkten • Leg de acties van de genomen maatregelen vast in het dossier	Contactpersoon Datalekken

4.Vaststellen impact datalek	• Onderzoek het datalek en de gevolgen daarvan • Onderzoek de aard van de gegevens die gelekt zijn. Bijv. gezondheidsgegevens, wachtwoorden, gegevens over financiële situatie of die kunnen leiden tot stigmatisering/misbruik • Onderzoek de omvang van de gelekte gegevens • Beoordeel welke impact het lek kan hebben op de betrokken personen • Stel vast wat de nadelige gevolgen kunnen zijn	Contactpersoon Datalekken
5. Vaststellen Meld en Herstelaanpak	• Bepaal aanpak/informeren AP • Bepaal aanpak/informeren betrokkenen • Bepaal acties voor nazorg betrokkenen • Bepaal acties voor belang van de organisatie • Bepaal acties voor verbetering beveiliging	Contactpersoon Datalekken
6. Melden AP*	• Indien besloten wordt om AP te informeren dan moet dat binnen 72 uur • Melding via de website van het AP • Van tevoren kan het Meldformulier Datalekken gebruikt worden	Contactpersoon Datalekken
7. Melden betrokkenen**	• Melding via bijvoorbeeld brief • Meedelen wat er is gebeurd, welke persoonsgegevens getroffen zijn en wat de mogelijke gevolgen van het datalek kunnen zijn • Informeren over de maatregelen die de organisatie neemt en die de betrokkene zelf kan nemen om schade te voorkomen	Contactpersoon Datalekken
8. Uitvoeren herstelwerkzaamheden	• Herstel het datalek • Verbeteren van de beveiliging • Lever nazorg aan de betrokkenen	Contactpersoon Datalekken
9. Optimaliseer het beveiligings- en het Datalek proces	• Registreer, evalueer en verbeter de beveiliging en het proces inzake melding datalekken	Contactpersoon Datalekken

* Melding aan de Autoriteit persoonsgegevens kan alleen achterwege blijven indien het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen. Of hiervan sprake is hangt mede af van de aard en omvang van de gelekte persoonsgegevens.

** Indien het datalek waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen veroorzaakt, moet het datalek ook aan de betrokkenen gemeld worden. Het risico zal bijvoorbeeld moeten worden beoordeeld aan de hand van de aard en de hoeveelheid van de gelekte gegevens.

VERWERKER

Het kan gebeuren dat het datalek optreedt bij een verwerker. [BEDRIJFSNAAM] is en blijft (als verwerkingsverantwoordelijke) altijd verantwoordelijk voor het datalek bij de verwerker. In dat geval zal dus hetzelfde stappenplan worden afgewerkt. De verwerker zal bij de stappen betrokken worden.
Via de verwerkersovereenkomst moet afgedwongen worden dat de verwerker eventuele datalekken terstond (binnen 24 uur) meldt bij [BEDRIJFSNAAM] en [BEDRIJFSNAAM] helpt bij het beoordelen of er gemeld moet worden en de afwikkeling van het datalek. De verwerker wordt verwacht niet buiten [BEDRIJFSNAAM] om een datalek te melden bij de Autoriteit Persoonsgegevens. De verwerker moet verder alle redelijke instructies van de [BEDRIJFSNAAM] opvolgen.

CONSEQUENTIES VAN NON-COMPLIANCE

De AVG stelt strenge eisen aan de melding en de registratie van datalekken. Organisaties moeten alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of een organisatie aan de meldplicht datalekken heeft voldaan. Is dit niet mogelijk dan is de organisatie in overtreding van de wet AVG.

Heeft u hulp nodig bij het opstellen van uw Protocol Datalekken?
TT3P helpt u graag. Neem contact met ons op!

Hofplein 20 • 3022 AC Rotterdam • 088 38 38 38 3 • info@tt3p.nl • www.tt3p.nl