Bijlage 11

Afspraken betreffende inbreuken in verband met persoonsgegevens

Een nieuwe/vermoedelijke melding doen
Conform de AVG wet- en regelgeving dient ICTU datalekken **binnen 72 uur** te melden bij de Autoriteit Persoonsgegevens (AP). Hierbij kan er ook een voorlopige melding gedaan worden, indien nog niet alles bekend is of indien ICTU twijfelt of het een datalek is. Het is derhalve van belang dat (sub)verwerkers een (vermoeden van) een datalek **uiterlijk binnen 36 uur** melden bij ICTU Security Center via dit formulier met cc naar de contactpersoon van de opdrachtgever.

NB: ook **vermoedens van een datalek** dienen aan ICTU gemeld te worden.

ICTU Security Center is bereikbaar via **privacy@ictu.nl**

Na ontvangst van het formulier voert het DBV-Security Center een analyse uit om te bepalen of het een datalek is en neemt hiervoor waar nodig contact op met de (sub)verwerker. Dit betekent dat de melding niet automatisch wordt doorgezet naar de AP.

Let op! Graag alle velden invullen ook al weet je het antwoord niet. Maak de beste keuze en geef ons een toelichting onder aan het formulier. Voor de melding aan de AP zijn veel van deze velden verplicht vandaar het verzoek alle vragen altijd te beantwoorden.

1 Melding Datalek door (sub)verwerker

Let op: Deze velden zijn verplicht. Zelfs indien er (nog)geen juist antwoord mogelijk is. Probeer deze dan het meest accuraat te beantwoorden.

1.1 Wie meldt het datalek en is de contactpersoon?

Naam

Functie

E-mailadres

Telefoonnummer

Organisatie

1.1.1 Betrokkenheid andere organisatie

Was er een andere organisatie(sub verwerker) betrokken bij de inbreuk?

Kies er een

Naam van de andere organisatie die betrokken was bij de inbreuk

In welke hoedanigheid was de andere organisatie betrokken bij de inbreuk?

1.2 Tijdlijn

Exacte datum waarop de inbreuk was, indien bekend

Startdatum van de periode waarbinnen de inbreuk was

Einddatum van de periode waarbinnen de inbreuk was

Duurt de inbreuk op dit moment nog voort?

Kies er een

Wanneer werd de inbreuk ontdekt?

Als u de inbreuk later meldt dan 24 uur na de ontdekking, wat is daarvan dan de reden?

1.3 Gegevens over het datalek

1.3.1 Aard van de inbreuk

Inbreuk op de vertrouwelijkheid van de gegevens

Kies er een

Inbreuk op de integriteit van de gegevens

Kies er een

Inbreuk op de beschikbaarheid van de gegevens

Kies er een

1.3.2 Aard van het incident

Wat is de aard van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest?

Kies er een

Geef een samenvatting van het incident waarbij er een inbreuk op de beveiliging van persoonsgegevens is geweest

1.4 Persoonsgegevens die betrokken zijn bij het datalek

1.4.1 Persoonsgegevens in het algemeen

Naam
Kies er een
Geslacht, geboortedatum en/of leeftijd
Kies er een
Burgerservicenummer (BSN)
Kies er een
Contactgegevens
Kies er een
Toegangs- of identificatiegegevens
Kies er een
Financiële gegevens
Kies er een
(Kopieën van) paspoorten of andere legitimatiebewijzen
Kies er een
Locatiegegevens
Kies er een
Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen
Kies er een
Onbekend / anders, namelijk:

1.4.2 Bijzondere categorieën van persoonsgegevens

Persoonsgegevens waaruit iemands ras of etnische afkomst blijkt
Kies er een
Persoonsgegevens waaruit iemands politieke opvattingen blijken
Kies er een
Persoonsgegevens waaruit iemands religieuze of levensbeschouwelijke overtuigingen blijken
Kies er een
Persoonsgegevens waaruit iemands lidmaatschap van een vakbond blijkt
Kies er een
Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid
Kies er een
Gegevens over iemands gezondheid
Kies er een
Genetische gegevens
Kies er een
Biometrische gegevens
Kies er een

1.4.3 Hoeveelheid persoonsgegevens

Geef (eventueel bij benadering) aan hoeveel gegevensrecords ("gegevensregisters") zijn getroffen door de inbreuk

1.5 De groep mensen van wie persoonsgegevens betrokken zijn bij het datalek

Werknemers

Kies er een

Klanten (huidig en potentieel)

Kies er een

Leerlingen of studenten

Kies er een

Patiënten

Kies er een

Minderjarigen

Kies er een

Personen uit kwetsbare groepen

Kies er een

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk.

Van minimaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

Van maximaal hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

1.6 Maatregelen die zijn getroffen voordat het datalek plaatsvond

Waren de persoonsgegevens op het moment dat de inbreuk zich voordeed versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk voor onbevoegden?

Kies er een

Als de persoonsgegevens deels onbegrijpelijk of ontoegankelijk waren, om welk deel gaat

Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk waren gemaakt, op welke manier is dit dan gebeurd?

1.7 Gevolgen van het datalek

1.7.1 Gevolgen van de inbreuk op de vertrouwelijkheid, de integriteit en/of de beschikbaarheid van de gegevens.

Onbevoegden hebben kennis kunnen nemen van de gegevens

Kies er een

De gegevens kunnen op een onbehoorlijke of onrechtmatige manier worden misbruikt

Kies er een

Er worden binnen uw eigen organisatie mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens gebruikt

Kies er een

Er worden mogelijk onjuiste, onvolledige of achterhaalde persoonsgegevens hergebruikt voor andere doeleinden of doorgegeven aan andere organisaties

Kies er een

Een essentiële dienst kan tijdelijk niet meer worden verleend aan de betrokkenen

Kies er een

Een essentiële dienst kan permanent niet meer worden verleend aan de betrokkenen

Kies er een

Anders, namelijk

1.7.2 Lichamelijke, materiële en immateriële schade voor de betrokkenen

Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen?

Discriminatie

Kies er een

Identiteitsdiefstal of -fraude

Kies er een

Financiële verliezen

Kies er een

Reputatieschade

Kies er een

Verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens

Kies er een

Ongeoorloofde ongedaan making van pseudonimisering

Kies er een

Betrokkenen kunnen hun rechten en vrijheden niet uitoefenen

Kies er een

Betrokkenen worden verhinderd controle over hun persoonsgegevens uit te oefenen

Kies er een

Andere gevolgen, namelijk:

Geef een inschatting van de ernst van de mogelijke gevolgen voor de betrokkenen

Kies er een

1.8 Vervolgacties naar aanleiding van het datalek

1.8.1 Maatregelen om de inbreuk aan te pakken

Welke technische en organisatorische maatregelen heeft uw organisatie getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

1.8.2 Informeren van partijen, heeft u betrokken en/of andere partijen geïnformeerd?

1.8.3 Internationale aspecten

In welke landen heeft de inbreuk zich voorgedaan?

1.8.4 Overige informatie welke bruikbaar zou kunnen zijn:

Voorzie ons waar mogelijk van informatie die van belang is of zou kunnen zijn voor eventueel vervolg onderzoek en waar niet naar is gevraagd of waar onvoldoende ruimte was om te antwoorden in de voorgaande vragen.

Verstuur dit formulier naar Privacy@ictu.nl met cc naar de contactpersoon van de opdrachtgever na het ontdekken van een datalek. Altijd zo spoedig mogelijk, en nooit later dan 24 uur na het ontdekken van het datalek!