Protocol datalekken

1 Begrippen

Persoonsgegevens:

Iedere informatie die herleidbaar is tot een levende natuurlijke persoon, ofwel iemand moet door deze informatie direct geïdentificeerd worden of indirect identificeerbaar zijn. Het gaat daarbij om objectieve gegevens: naam, voornamen, voorletters, geslacht, geboortedatum, (e-mail)adres, postcode, woonplaats, telefoonnummer, bankrekeningnummer, beroep, inkomensgegevens, autokenteken, hoogte kinderopvangtoeslag, eventuele betalingsachterstand. Ook subjectieve informatie valt hieronder, zoals meningen en oordelen over betrokkene of de wetenschap dat iemand een dubieuze debiteur of op korte termijn zal overlijden.

Bijzondere persoonsgegevens:

Gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven of lidmaatschap van een vakvereniging. Ook strafrechtelijke gegevens en persoonsgegevens over hinderlijk of onrechtmatig gedrag (hennep, overlast, etc), waarvoor een veroordeling of verbod is opgelegd behoren hiertoe.

Verwerken:

Alle handelingen (zowel geautomatiseerd als niet-geautomatiseerd) die betrekking hebben op persoonsgegevens. Het gaat dan om o.a. verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, ter beschikking stellen, uitwissen en vernietigen.

Verantwoordelijke:

Degene die het doel van en de (financiële) middelen voor de verwerking van persoonsgegevens vaststelt. De directeur is Verantwoordelijke.

Verwerker:

Degene die ten behoeve van de Verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreekse gezag te zijn onderworpen.

Autoriteit Persoonsgegevens:

Een overheidsinstantie die toeziet op een zorgvuldig gebruik van persoonsgegevens. Voorheen CBP.

Datalek:

Van een datalek wordt gesproken als persoonsgegevens in handen vallen van derden die geen toegangtot die gegevens mogen hebben. Een datalek is het gevolg van een beveiligings-probleem en kan plaatsvinden bij Coöperatie Mbo Voorzieningen U.A. zelf of bij een van zijn Verwerkers.

2 Inleiding

In dit protocol beschrijven we hoe te handelen op het moment dat een datalek zich bij de Coöperatie Mbo Voorzieningen U.A.. als verantwoordelijke, of bij een van onze verwerkers zich voor doet.

Versie	**Datum**	**Gewijzigd**	**Naam**
1.0	19 mei 2021	Eerste officiële versie	PV

Inhoudsopgave

3 Doel en afbakening

Doel van het protocol: een goed werkbaar plan dat:

- Coöperatie Mbo Voorzieningen U.A. helpt bij het efficiënt en effectief oplossen van een datalek
- waarbij wordt voldaan aan de wetgeving op dit gebied;
- dat zicht geeft op de verdeling van taken en rollen van betrokkenen;
- en dat zorgt voor de juiste afwikkeling van een datalek zodra dat plaatsvindt bij Coöperatie Mbo Voorzieningen U.A. of bij een van zijn (sub) verwerkers.

Dit protocol bevat een draaiboek met daarin een beslisboom die verder gaat dan alleen de techniek dan wel het in stand houden van de dienstverlening. Ook de onderwerpen schade aan derden, aansprakelijkheid en communicatie zijn meegenomen.

Met dit plan sluiten we zoveel als mogelijk aan op reeds bestaande processen op het gebied van ICT-incidenten, communicatie en aansprakelijkheidstelling. We leggen deze afspraken en processen niet als zodanig vast in dit draaiboek. Mogelijke aanpassingen in deze processen in de toekomst hebben daarmee geen directe gevolgen voor dit protocol.

3.1 Toepassing protocol

Dit protocol is voor Coöperatie Mbo Voorzieningen U.A. de leidraad die gebruikt wordt bij het omgaan met datalekken die gevolgen (kunnen) hebben voor de privacy van studenten van de leden van de Coöperatie Mb Voorzieningen U.A.

3.2 Systematiek en procedure

3.2.1 Melding

Computer datalek
Een computer datalek wordt als incident gemeld bij de info@mbovoorzieningen.nl of support@mbovoorzieningen.nl . Hier wordt een eerste beoordeling van de melding gedaan en wordt bepaald of het daadwerkelijk een datalek betreft. Indien het een datalek betreft dan wordt de FG op de hoogte gesteld. Deze informeert het team Datalekken (zie 5.2).

3.2.2 Systematiek Risico-inschatting

Het team Datalekken start een onderzoek naar het datalek waarbij het volgende wordt onderzocht:
Welke inbreuk op de beveiligingsmaatregelen heeft plaatsgevonden (Bijv. een hack of verlies van gegevens) en wanneer;

- Welk onderdeel van de IT-systemen betrokken is (website of database) en/of welke apparatuur en waar deze verloren is gegaan of is gestolen;
- Welke persoonsgegevens mogelijk betrokken zijn;
- Wat de (verwachte) consequenties van het datalek zijn;
- Welke maatregelen genomen kunnen worden om de beveiliging te herstellen;

De Contactpersoon belegt zo spoedig mogelijk een vergadering. Buiten de reguliere werktijden kan dit telefonisch worden afgehandeld. Op basis van de uitkomsten van het onderzoek wordt afgewogen of een melding aan de Toezichthouder noodzakelijk is. Als een datalek namelijk leidt tot ernstige nadelige

gevolgen voor de bescherming van persoonsgegevens (of als een aanzienlijke kans bestaat dat dit gebeurt) moet het datalek binnen 72 uur gemeld worden bij de Autoriteit Persoonsgegevens.
Deze afweging is maatwerk en onder meer afhankelijk van de volgende voorwaarden:

Er is sprake van een inbreuk op de beveiliging van persoonsgegevens;
De inbreuk leidt tot een aanmerkelijke kans op nadelige gevolgen voor de bescherming van de persoonsgegevens die door de organisatie wordt verwerkt.

Als aan bovenstaande voorwaarden is voldaan dan is de meldplicht aan de Toezichthouder van toepassing. Zie Procedure 1 onder 4.4.1.

Als daarnaast ook nog aan de volgende voorwaarde is voldaan:

De inbreuk leidt tot nadelige gevolgen voor de persoonsgegevens en persoonlijke levenssfeer van de betrokkenen, dan is de meldplicht aan de Autoriteit Persoonsgegevens en aan de betrokken personen van toepassing. Zie Procedure 2 onder 4.4.2.

Melding aan de Toezichthouder en betrokkenen kan achterwege blijven als de betreffende persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor een ieder die geen recht heeft op kennisname van de gegevens. (Encryptie)
Een passende versleuteling van persoonsgegevens bij een beveiligingslek geeft geen gevaar voor ernstig nadelige gevolgen voor de privacy van de betrokkenen. De teamleider automatisering is verantwoordelijk voor de beoordeling of voldaan is aan dit criterium van onbegrijpelijkheid of ontoegankelijkheid voor derden. Bij twijfel is melding aan de Toezichthouder aan te bevelen.

Op Coöperatie Mbo Voorzieningen U.A. rust de verplichting om in de Verwerkersovereenkomsten met de Verwerkers een vergelijkbare meldplicht op te nemen die er op neerkomt dat de Verwerker Coöperatie Mbo Voorzieningen U.A. informeert indien er sprake is van een datalek.

4 Procedures Datalekken

4.1 Procedure 1: Melding van een datalek bij de AP

Het datalek is het gevolg van een inbreuk op de beveiliging van persoonsgegevens en de verwerkte persoonsgegevens zijn blootgesteld aan een aanmerkelijk risico van verlies of onrechtmatige verwerking.

De FG van de coöperatie belegt een vergadering met het team datalekken.
De FG stelt in overleg met het team datalekken in principe onverwijld maar in ieder geval binnen twee werkdagen de melding op en draagt zorg voor de melding richting de Toezichthouder (AP) met daarin in ieder geval:
De aard van de inbreuk;
De aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken;
Een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de in breuk voor de verwerking van de persoonsgegevens;

De maatregelen die de organisatie heeft genomen of voorstelt te nemen om deze gevolgen te verhelpen;
Als er niet binnen twee werkdagen bij de Toezichthouder een melding is gedaan wordt er in de melding beargumenteerd waarom dit niet is gebeurd.
Of ook de betrokkenen van de inbreuk in kennis worden gesteld;
De medewerker(s) waar meer informatie over de inbreuk kan worden verkregen

Indien zich een strafbaar feit heeft voorgedaan doet de FG aangifte
bij de politie van de hack of de diefstal van gegevens
De coöperatie stelt indien noodzakelijk een persbericht op en voert het communicatieplan uit.
De FG vult het register datalekken in.
Het team datalekken onderzoekt en lost het ICT datalek op.

4.2 Procedure 2: Melding van een datalek bij het AP en de betrokken personen

Het datalek is het gevolg van een inbreuk op de beveiliging van persoonsgegevens, de verwerkte persoonsgegevens zijn blootgesteld aan een aanmerkelijk risico van verlies of onrechtmatige verwerking en leidt tot nadelige gevolgen voor de persoonsgegevens en de persoonlijke levenssfeer van de betrokkenen.

De FG belegt een vergadering met het team datalekken.
De FG stelt in overleg met het team datalekken in principe onverwijld maar
in ieder geval binnen twee werkdagen de melding op en draagt zorg voor de melding richting de Autoriteit Persoonsgegevens met daarin in ieder geval:
De aard van de inbreuk;
De aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken;
Een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van de persoonsgegevens;
De maatregelen die de organisatie heeft genomen of voorstelt te nemen om deze gevolgen te verhelpen;
Of ook de betrokkenen van de inbreuk in kennis worden gesteld;
De medewerker(s) waar meer informatie over de inbreuk kan worden verkregen

- De FG stelt in overleg met het team datalekken de melding op richting de betrokken personen met daarin in ieder geval:
    - De aard van de inbreuk;
    - De instanties waar meer informatie over de inbreuk kan worden verkregen
    - De aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken
- De coöperatie informeert de betrokken personen per brief
- Indien zich een strafbaar feit heeft voorgedaan doet de controller aangifte bij de politie van de hack of de diefstal van gegevens. De Coöperatie stelt indien noodzakelijk een persbericht op en voert het communicatieplan uit.
- De FG vult het register datalekken in.
- Het team datalekken onderzoekt en lost het datalek op.

4.2.1 Oplossen Datalek

Naar aanleiding van de melding van een datalek heeft het team datalekken een onderzoek uitgevoerd naar de volgende punten:

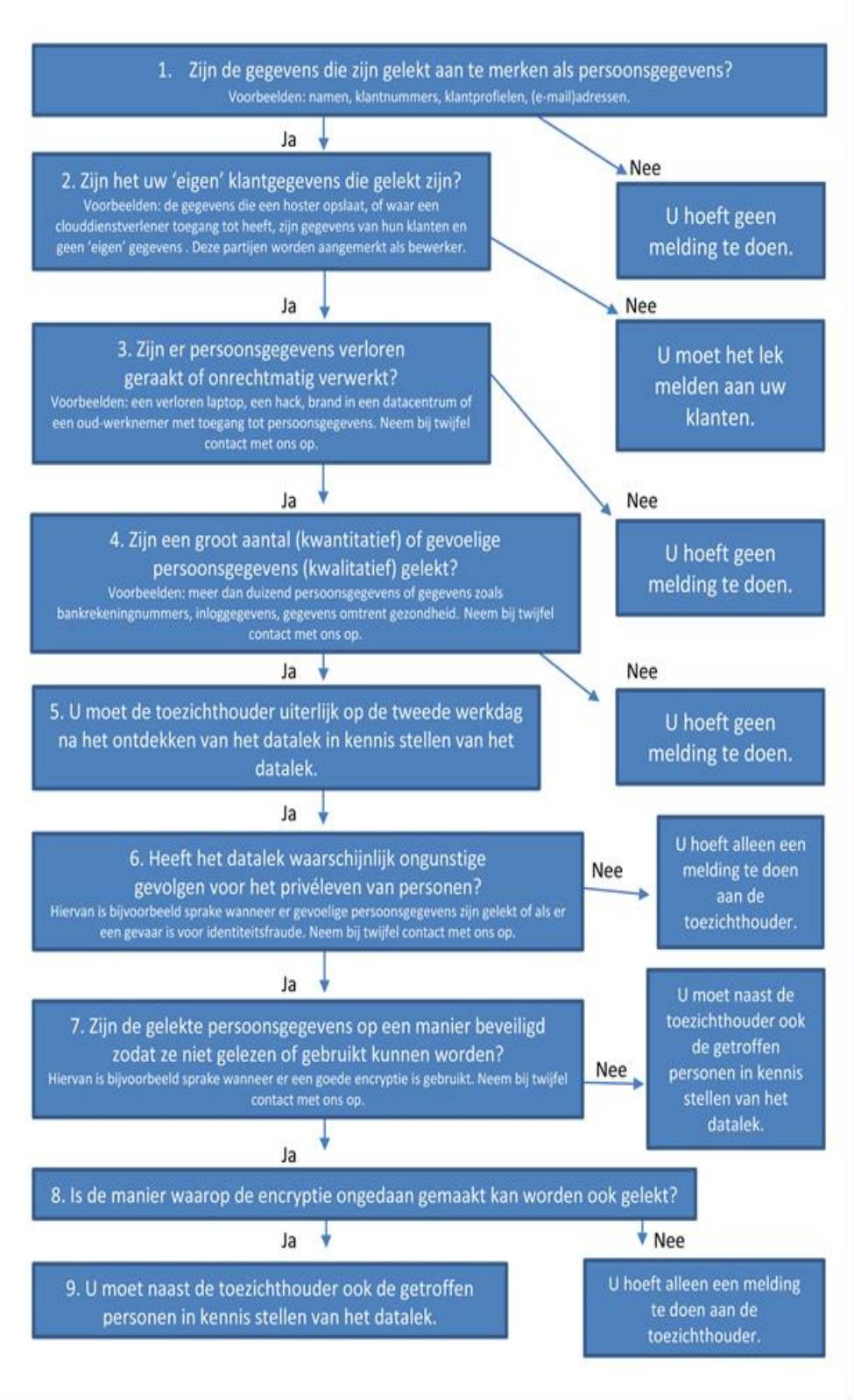
- Welke inbreuk op de beveiligingsmaatregelen heeft plaatsgevonden (Bijv. een hack of verlies van gegevens) en wanneer;
- Welk onderdeel van de IT-systemen is betrokken (website of database) en/of welke apparatuur en waar is deze verloren gegaan of gestolen;
- besluiten of de gebeurtenis behoort te worden geclassificeerd als informatiebeveiligingsincident;
- Welke persoonsgegevens zijn mogelijk betrokken
- Wat zijn de (verwachte) consequenties van het datalek
- Welke maatregelen kunnen worden genomen om de beveiliging te herstellen;

Het team datalekken richt zich op de bestrijding van het datalek (inclusief mogelijke reparatie van de ICT-omgeving) en zal bij het oplossen van het datalek vooral werken vanuit bestaande (ICT-)processen, waarbij de nadruk ligt op het classificeren, beoordelen, het beheersen en het oplossen van het datalek.

Gezien het belang van adequate communicatie naar de klanten, medewerkers of stakeholders, is het belangrijk om hier de nadruk op te leggen in deze fase, naast het oplossen van het datalek.

4.3 Beslisboom

De beschrijving van de procedure uit paragraaf 4.3.2 is in onderstaand figuur als beslisboom vormgegeven.



5 Team Datalekken

5.1 Inleiding

In dit hoofdstuk wordt de organisatie rondom het afhandelen van een datalek beschreven.

5.2 Team datalekken

Het (ad hoc) team datalekken bestaat uit:

Rol	Functie
Contactpersoon datalekken	FG
Team datalekken	FG, Algemeen Manager coöperatie, bestuur, producteigenaar
Verantwoordelijke	Bestuur

5.3 Team datalekken

Het team datalekken neemt beslissingen ten aanzien van het (bestrijding van het) datalek en verzorgt de communicatie naar belanghebbenden.

5.3.1 Taken van het team datalekken zijn onder andere:

- Besluiten of er sprake is van een datalek waarvoor een melding aan de Toezichthouder (AP) noodzakelijk is;
- Besluiten of er sprake is van een datalek waarvoor een melding aan de Toezichthouder (AP) en de betrokken personen noodzakelijk is;
- informeren van direct betrokkenen en andere belanghebbenden;
- het voorbereiden en eventueel zorgdragen voor mediavoorlichting;
- het eventueel opstellen van voortgangsrapportages;
- het fungeren als aanspreekpunt voor de FG van verwerkers en leden.

5.3.2 De rollen die minimaal in het team datalekken moeten worden ingevuld vertegenwoordigen het proces en de communicatie.

De Contactpersoon van het team datalekken is primair verantwoordelijk voor de samenstelling en het oproepen van het team. De Contactpersoon is daarnaast verantwoordelijk voor:

- het leiden van vergaderingen;
- het functioneren van het team datalekken;
- het nemen van besluiten;
- het eventueel doen van de melding aan de Toezichthouder (AP).

De directie van de coöperatie is verantwoordelijk voor:

- het helpen formuleren van de melding aan de Toezichthouder (AP);

- het helpen formuleren en doen van de melding aan de betrokken personen;
- de keuze en de inzet van de communicatiemiddelen zodat de boodschap de betreffende doelgroepen bereikt;
- perswoordvoering;
- het bewaken dat communicatie en voorlichting geschiedt conform daartoe geldende kaders;
- het uitbreiden van de communicatiecapaciteit, mocht de situatie daar om vragen;
- het informeren van direct betrokkenen en andere belanghebbenden. Daarnaast kan het team datalekken worden aangevuld met een adviseur of administratieve ondersteuning.

5.4 Communicatie en voorlichting

Bij een datalek is er veel behoefte aan goede informatie. De mate waarin gecommuniceerd wordt, hangt zoals beschreven in voorgaande alinea's, veelal af van de aard, ernst en gevolgen van het datalek en is daarbij dus ook afhankelijk van de coördinatiefase.

De communicatie richt zich op verschillende doelgroepen:
Interne communicatie: communicatie aan eigen medewerkers, inclusief directie en bestuur.
Externe communicatie: communicatie met de klanten, stakeholders, betrokken bedrijven en media.

Communicatie en voorlichting kan per datalek verschillen en moet voldoen aan de op dat moment geldende kaders. De medewerker beleid en communicatie in het team datalekken is ervoor verantwoordelijk dat binnen deze kaders gewerkt wordt.

6 Nazorg en kwaliteitsborging

6.1 Inleiding

Met nazorg worden alle activiteiten bedoeld die noodzakelijk zijn om voor afwikkeling van het datalek te zorgen, zoals het aansprakelijkheidsvraagstuk en een uit te voeren evaluatie en het borgen van het protocol datalekken in de processen van de organisatie.

6.2 Aansprakelijkheid

Werkzaamheden die tijdens en na het datalek worden uitgevoerd, brengen kosten met zich mee. In principe zijn de kosten die gemoeid zijn met deze werkzaamheden verhaalbaar op de veroorzaker. Om het mogelijk te maken om deze kosten te verhalen, moet er tijdens de bestrijding van het datalek informatie worden verzameld om de gemaakte kosten te kunnen aantonen. Indien er sprake is van verwijtbare schuld, dan dient tevens aangifte hiervan te worden gedaan bij de politie.

Daarnaast is het ook mogelijk dat Coöperatie Mbo Voorzieningen U.A. aansprakelijk worden gesteld voor geleden schade bij derden naar aanleiding van een datalek. Deze aansprakelijkstelling wordt conform de geldende procedure afgehandeld. Hierbij wordt minimaal onderzocht:

- Of de aansprakelijkstelling voldoende onderbouwd is;
- bij wie de schuld ligt;
- of schade te verhalen valt, of
- beroep kan worden gedaan op verzekeringen die door Coöperatie Mbo Voorzieningen U.A. zijn afgesloten.

6.3 Evaluatie

Bij datalekken die Procedure 1 en/ of 2 hebben doorlopen, moet een evaluatie plaatsvinden. Deze evaluatie heeft minimaal aandacht voor de volgende aspecten:

- de omstandigheden als gevolg waarvan het datalek kon optreden;
- de gekozen oplossing;
- de uitgevoerde werkzaamheden;
- eventuele noodzakelijke vervolgwerkzaamheden;
- de gehanteerde werkwijze;
- de verrichte communicatieacties;
- de noodzakelijke aanpassingen voor het protocol datalekken;
- financiële gevolgen van het datalek;
- gevolgen en acties op het gebied van aansprakelijkheid.

6.4 Forensisch bewijs

Hierbij moet ook rekening worden gehouden met eventueel forensisch bewijs
Er behoort rekening te worden gehouden met de:

- bewakingsketen;
- veiligheid van bewijs;
- veiligheid van personeel;
- rollen en verantwoordelijkheden van het betrokken personeel;
- competentie van personeel;
- documentatie;
- instructie.

Indien beschikbaar, behoort certificatie of andere relevante methoden om personeel en middelen te kwalificeren te worden gezocht om de waarde van het verkregen bewijs te versterken.
Forensisch bewijs kan grenzen van organisaties of rechtsgebieden overschrijden. In zulke gevallen behoort te worden gewaarborgd dat de organisatie het recht heeft de vereiste informatie als forensisch bewijs te verzamelen. De eisen van verschillende rechtsgebieden behoren ook in aanmerking te worden genomen om de kans zo groot mogelijk te maken dat het bewijs wordt toegelaten in de relevante rechtsgebieden.

6.5 Onderhoud van het Protocol

6.5.1 Planmatig onderhoud

Het protocol datalekken dient up-to-date te worden gehouden door periodieke controle van de inhoud van het protocol. Het actualiseren van dit protocol datalekken wordt in de toekomst meegenomen in de cyclus voor het actualiseren van het Informatiebeveiligingsplan.

6.5.2 Niet-planmatig onderhoud

Regulier onderhoud van het protocol datalekken vindt plaats als uitgevoerde evaluaties naar aanleiding van datalekken hiertoe aanleiding geven. Dit onderhoud vindt plaats op basis van aanpassingsvoorstellen.

7 Bijlage 1 Vragenlijst AP Meldplicht Datalekken

Dit formulier dient volledig te worden ingevuld en daarna ingezonden te worden naar de AP.

1. Aard van de melding

Is dit een vervolg op een eerdere melding? (Kies een van de volgende opties.)

a) Ja
b) Nee

2. Wat is het nummer van de oorspronkelijke melding? (Beantwoord deze vraag als u vraag 1 met ja hebt beantwoord.)

3. Wat is de strekking van de vervolgmelding? (Beantwoord deze vraag als u vraag 1 met ja hebt beantwoord, kies een van de volgende opties.)
    a) Toevoegen of wijzigen van informatie betreffende de eerdere melding
    b) Intrekking van de eerdere melding

4. Wat is de reden van intrekking? (Beantwoord deze vraag als u bij vraag 3 gekozen heeft voor optie b.)

5. Op grond van welke wettelijke bepaling doet u deze melding?
    a) artikel 33 van de AVG
    b) artikel 11.3a, eerste lid, van de Tw

6. Over welk bedrijf of welke organisatie gaat het? (Vul de onderstaande gegevens in.)
    - Naam van het bedrijf of de organisatie
    - (Bezoek)adres
    - Postcode
    - Plaats
    - KvK-nummer

7. Door wie wordt het datalek gemeld? (Vul de onderstaande gegevens in.)
    - Naam van de persoon die meldt
    - Functie van de persoon die meldt
    - E-mailadres van de persoon die meldt
    - Telefoonnummer van de persoon die meldt
    - Alternatief telefoonnummer van de persoon die meldt

8. Met wie kan het AP contact opnemen voor nadere informatie over de melding? (Vul de onderstaande gegevens in indien dit iemand anders is dan de melder van het datalek.)
    - Naam contactpersoon
    - Functie van de contactpersoon

- E-mailadres van de contactpersoon
- Telefoonnummer van de contactpersoon
- Alternatief telefoonnummer van de contactpersoon

9. In welke sector is het bedrijf of de organisatie actief?

10. Gegevens over het datalek

Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.

11. Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk? (Vul de aantallen in.)
    Minimaal: (vul aan)
    Maximaal: (vul aan)

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

13. Wanneer vond de inbreuk plaats? (Kies een van de volgende opties en vul waar nodig aan.)
    Op (datum)
    Tussen (begindatum periode) en (einddatum periode)
    Nog niet bekend

Wat is de aard van de inbreuk? (U kunt meerdere mogelijkheden aankruisen.)

Lezen (vertrouwelijkheid)
Kopiëren
Veranderen (integriteit)
Verwijderen of vernietigen (beschikbaarheid)
Diefstal
Nog niet bekend

Om welk type persoonsgegevens gaat het? (U kunt meerder mogelijkheden aankruisen.)

Naam-, adres- en woonplaatsgegevens
Telefoonnummers
E-mailadressen of andere adressen voor elektronische communicatie
Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam / wachtwoord of klantnummer)
Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)
Burgerservicenummer (BSN) of sofinummer
Paspoortkopieën of kopieën van andere legitimatiebewijzen
Geslacht, geboortedatum en/of leeftijd
Bijzondere persoonsgegevens (bijvoorbeeld ras, etniciteit, criminele gegevens, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, medische gegevens)
Overige gegevens, namelijk (vul aan)

14. Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokkenen? (U kunt meerdere mogelijkheden aankruisen.)
    Stigmatisering of uitsluiting
    Schade aan de gezondheid
    Blootstelling aan (identiteits)fraude
    Blootstelling aan spam of phishing
    Anders, namelijk (vul aan)

15. Vervolgacties naar aanleiding van het datalek

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

16. Inlichten van de betrokkenen

Heeft u het datalek gemeld aan de betrokkenen of bent u van plan dat te gaan doen? (Kies een van de volgende opties.)

a) Ja
Nee
Nog niet bekend

17. Wanneer heeft u het datalek gemeld aan de betrokkenen, of wanneer gaat u dit doen? (Beantwoord deze vraag als u vraag 20 met ja hebt beantwoord. Kies een van de volgende opties en vul waar nodig aan.)
    Ik heb het datalek aan de betrokkenen gemeld op (datum)
    Ik ga het datalek aan de betrokkenen melden op (datum)
    Nog niet bekend

18. Wat is de inhoud van de melding aan de betrokkenen? (Letterlijke weergave, beantwoord deze vraag als u vraag 18 met ja hebt beantwoord.)

19. Hoe veel betrokkenen heeft u in kennis gesteld of gaat u in kennis stellen? (Beantwoord deze vraag als u vraag 18 met ja hebt beantwoord.)

20. Welk communicatiemiddel of welke communicatiemiddelen gebruikt u of gaat u gebruiken bij het in kennis stellen van de betrokkenen? (Beantwoord deze vraag als u vraag 18 met ja hebt beantwoord.)

21. Waarom ziet u af van het melden van het datalek aan de betrokkenen? (Beantwoord deze vraag als u vraag 18 met nee hebt beantwoord. Kies een van de onderstaande opties en vul waar nodig aan.)
    De technische beschermingsmaatregelen die ik heb getroffen bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten
    Het is onwaarschijnlijk dat het datalek ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, want: (vul aan)
    Ik heb zwaarwegende redenen om de melding aan de betrokkene achterwege te laten, namelijk: (vul aan)

Anders, namelijk: (vul aan)

22. Technische beschermingsmaatregelen

Zijn de persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden? (Kies een van de volgende opties en vul waar nodig aan.)

Ja

Nee

Deels, namelijk: (vul aan)

23. Als de persoonsgegevens geheel of deels onbegrijpelijk of ontoegankelijk zijn gemaakt op welke manier is dit dan gebeurd? (Beantwoord deze vraag als u bij vraag 24 heeft gekozen voor optie a of optie c. Als u gebruik heeft gemaakt van encryptie, licht dan ook de wijze van versleutelen toe.)

24. Internationale aspecten

Heeft de inbreuk betrekking op personen in andere EU-landen? (Kies een van de volgende opties.)

Ja

Nee

Nog niet bekend

25. Heeft uw bedrijf of organisatie het datalek gemeld bij toezichthouders in een of meer andere EU-landen?

Ja, namelijk: (vul aan)

Nee

26. Vervolgmelding

Is naar uw mening deze melding compleet? (Selecteer een van onderstaande opties.)

Ja, de vereiste informatie is verstrekt en er is geen vervolgmelding nodig

Nee, er komt later een vervolgmelding met aanvullende informatie over deze inbreuk.