Privacybeleid St. Regiobibliotheek Lek & IJssel

Algemeen

Ingangsdatum:	16 april 2018
Wijzigingsdatum:	5 mei 2022
Versie:	1.3
Opgesteld door:	Gert Staal, directeur-bestuurder
Vastgesteld op:	3 mei 2022 door MT en directie
Ondertekening:	Gert Staal, 3 mei 2022

Inleiding

Dit Privacybeleid heeft betrekking op de bescherming van persoonsgegevens van alle betrokkenen van BLIJ. Het gaat hier in ieder geval om alle medewerkers, de klanten (leden), bezoekers en externe relaties.

Om ervoor te zorgen dat BLIJ kan voldoen aan relevante wet- en regelgeving, is het belangrijk dat alle medewerkers op de hoogte zijn van het Privacybeleid. Het Privacybeleid helpt – met de juiste acties – veilig met persoonsgegevens om te gaan. Door het weergeven van taken, bevoegdheden en verantwoordelijkheden is het voor een ieder duidelijk wat zijn of haar taak is binnen BLIJ. Uiteindelijk is elke medewerker verantwoordelijk voor een juiste omgang met persoonsgegevens.
Het doel van dit Privacybeleid is om de kwaliteit van de gegevensverwerking te optimaliseren, waarbij we zoeken naar een goede balans tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de privacy van de betrokkenen wordt gerespecteerd. De gegevensverwerking moet voldoen aan relevante wet- en regelgeving.
Het Privacybeleid beschrijft op strategisch niveau de doelstellingen op het gebied van de bescherming van persoonsgegevens. Het geeft op die manier richting aan de gehele organisatie als het gaat om de verwerking van persoonsgegevens. Voor organisatieonderdelen en aparte diensten gelden operationele kaders binnen het strategisch beleid.

Met de invoering van de Algemene verordening gegevensbescherming (AVG) op 25 mei 2018 werd een nieuw Privacybeleid ingevoerd. Het document beschrijft in vogelvlucht onze uitgangspunten, taken en bevoegdheden in de organisatie, algemene beginselen van de bescherming van persoonsgegevens, verwerking van persoonsgegevens, rechtmatigheid, bewaartermijn, verwerkingsregister, Gegevensbeschermingseffectbeoordeling (GEB), rechten van betrokkenen, verwerkers, hoe wij gegevens met anderen delen, hoe we omgaan met informatiebeveiliging en datalekken, wie de Functionaris gegevensbescherming is en hoe deze te bereiken valt, en hoe we wijzigingen zullen verwerken.

Taken en bevoegdheden binnen de organisatie

BLIJ heeft ervoor gekozen om een functionaris gegevensbescherming (FG) aan te stellen met als taak toezicht te houden op de naleving van de wet- en regelgeving op het gebied van de bescherming van persoonsgegevens, evenals toezicht op de uitvoering van dit Privacybeleid. De functionaris gegevensbescherming helpt bij de invoering van dit Privacybeleid. Alle medewerkers zijn verplicht om medewerking te verlenen aan de FG indien dit gevraagd wordt.

Er zijn binnen de organisatie drie afdelingen, t.w. Publieksservice, Programma's en Bedrijfsbureau, ieder aangestuurd door managers. De manager Bedrijfsbureau heeft de rol van Functionaris gegevensbescherming (gezien de omvang van de organisatie zijn dit rollen, geen functies). Het kan zijn dat deze rol op enig moment door BiSC wordt ingevuld.

Uitgangspunten

BLIJ vindt het belangrijk om transparant te handelen, vooral in het kader van de verwerking van persoonsgegevens. Daarom gaat BLIJ veilig en integer met de persoonsgegevens om en is handelt in overeenstemming met de wet- en regelgeving op het gebied van de bescherming van persoonsgegevens (Algemene verordening persoonsgegevens). Bij de werkzaamheden van BLIJ worden de algemene beginselen op het gebied van de verwerking van persoonsgegevens in acht genomen. Daarnaast worden alle medewerkers getraind op het gebied van privacy om ervoor te zorgen dat de bescherming van persoonsgegevens verzekerd kan worden. Ook zorgt BLIJ ervoor dat bij het ontwerpen van nieuw beleid, het inrichten van nieuwe processen of andere relevante zaken de begrippen *privacy by design* en *privacy by default* een rol speelt. BLIJ beperkt het verwerken van persoonsgegevens tot de uitdrukkelijk omschreven doelen waarvoor ze verzameld zijn. Daarbij wordt het vereiste van doelbinding nageleefd.

Voor het behandelen van de rechten van de betrokkenen is een procedure ingericht. Op deze manier kan BLIJ ervoor zorgen dat de betrokkenen hun rechten kunnen uitoefenen.
De persoonsgegevens worden in beginsel niet naar landen gestuurd buiten de Europese Unie. Wanneer er een noodzaak is om dit toch te doen, wordt deze noodzaak schriftelijk gemotiveerd.
De inventarisatie en actualisatie van het verwerkingsregister vindt periodiek plaats (minimaal 1 keer per kwartaal) en indien nodig wordt een gegevensbeschermingseffectbeoordeling gedaan (GEB) voor nieuwe of gewijzigde toepassingen.

<u>Algemene beginselen van de bescherming van persoonsgegevens</u>
De verwerking moet voldoen aan de algemene beginselen van de bescherming van persoonsgegevens. De verwerking van persoonsgegevens moet aan de volgende eisen voldoen:

- Verwerkingen moeten rechtmatig, eerlijk en transparant zijn ten opzichte van de betrokkenen.
- Persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld.
- Persoonsgegevens mogen niet verder worden verwerkt op een met die doeleinden onverenigbare wijze. Verenigbaar met het oorspronkelijke doel zijn verwerkingen voor archivering, doeleinden van algemeen belang, wetenschappelijke en historische onderzoeksdoeleinden en statistische doeleinden.
- Persoonsgegevens moeten adequaat en ter zake dienend zijn en beperkt blijven tot datgene wat minimaal nodig is voor de doeleinden waarvoor zij worden verwerkt.
- Persoonsgegevens moeten accuraat en waar nodig up-to-date zijn.
- Persoonsgegevens mogen niet langer worden bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren dan voor verwezenlijking van de doeleinden waarvoor ze worden verwerkt, noodzakelijk is. Persoonsgegevens mogen langer worden bewaard voor archivering in het algemeen belang en voor historische, statistische of wetenschappelijke doeleinden.
- Persoonsgegevens mogen alleen worden verwerkt op een manier die de veiligheid van de persoonsgegevens verzekert. Wanneer verwerking plaatsvindt op grond van gerechtvaardigd belang, één van de 6 wettelijke grondslagen, pas na een expliciete afweging van de gevolgen van de verwerking voor de belangen van de betrokkene en de belangen van de organisatie.

Het is belangrijk dat BLIJ kan aantonen dat aan deze beginselen wordt voldaan. Eén van de manieren om dit aan te tonen is door het vormgeven, implementeren en onderhouden van dit Privacybeleid. Daarnaast is de privacyverklaring – onder andere te vinden op de website van BLIJ - een manier om te voldoen aan de beginselen. Verder worden de werknemers getraind op privacy-bewustzijn en zijn processen ingericht om te voldoen aan de beginselen.

<u>Verwerking van persoonsgegevens</u>

Bijna alle medewerkers hebben dagelijks veel te maken met de verwerking van persoonsgegevens. Waar nodig kunnen voor sommige afdelingen aparte operationele handreikingen geschreven worden die specifiek gericht zijn op hun werkzaamheden waarbij aandacht wordt geschonken aan specifieke aspecten van het Privacybeleid (bijvoorbeeld maatregelen binnen BicatWISE), zie de bijlagen.

Rechtmatigheid
De organisatie doet een toets op de rechtmatigheid van verwerkingen gebaseerd op het model zoals dat door BiSC ter beschikking is gesteld, en heeft daarmee de rechtmatigheid van verwerkingen gecontroleerd.

Bewaartermijn
In beginsel, als uitgangspunt, worden alleen persoonsgegevens bewaard als dat voor de bedrijfsvoering noodzakelijk is. In beginsel worden persoonsgegevens bewaard met de termijnen, specifiek voor iedere verwerking genoemd in Bijlage 1. Verwerkingsregister BLIJ

Verwerkingsregister
De organisatie heeft een verwerkingsregister samengesteld gebaseerd op het model zoals dat door BiSC ter beschikking is gesteld. Deze zijn inzichtelijk voor alle medewerkers.
Zie Bijlage 1. Verwerkingsregister BLIJ.

Gegevensbeschermingseffectbeoordeling (GEB)
De organisatie heeft een Gegevensbeschermingseffectbeoordeling (GEB) opgesteld gebaseerd op het model zoals dat door BiSC ter beschikking is gesteld, voor die verwerkingen waar deze nodig zijn op basis van het Register Gegevensverwerkingen in Bijlage 1. Deze GEBs zijn inzichtelijk voor alle medewerkers via Workspace.

Rechten van betrokkenen
Er bestaat een regeling die de rechten van betrokkenen uiteenzetten voor medewerkers en voor klanten/gebruikers van de bibliotheek. (zie Workspace). Dit is de Privacyverklaring

Verwerkers
In het geval van verwerking door externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt BLIJ afspraken over de eisen waar de verwerking aan moet voldoen. Deze afspraken voldoen aan de wet. BLIJ controleert deze afspraken minimaal 1 keer per jaar op relevantie en actualiteit, in het eerste kwartaal van ieder jaar, en vermeldt resultaten van de controle in het bestuursverslag. Bij het aanstellen van een verwerker wordt een verwerkersovereenkomst gesloten. Deze overeenkomst wordt op basis van een standaardmodel opgemaakt (zie Workspace).

Delen van gegevens met anderen
Zowel intern als extern zijn wij te allen tijde voorzichtig met het delen van persoonsgegevens met anderen. We zijn ons bewust van het feit dat het delen van gegevens anderen nadeel of schade kan berokkenen. In beginsel delen wij alleen informatie op het moment dat dat a. wettelijk toegestaan is en b. een organisatiedoelstelling dient.

Informatiebeveiliging en datalekken
Als uitgangspunt dienen alle persoonsgegevens beveiligd te worden met passende technische en organisatorische maatregelen. Het beleid voor Informatiebeveiliging wordt apart beschreven in de Bijlage 5. Informatiebeveiligingsbeleid BiSC.

Datalekken dienen direct gemeld te worden bij de functionaris gegevensbescherming. Er is een procedure voor melding van datalekken ingesteld, zie Bijlage 6. Procedure melding datalekken. Er is

ook een meldformulier beschikbaar voor het melden van datalekken. Zie Bijlage 7. Meldformulier datalekken BLIJ.

Functionaris Gegevensbescherming

De rol van Functionaris Gegevensbescherming wordt ingevuld door de Controller, dhr. Rien Hageman, rienhageman@bibliotheeklekijssel.nl, mobiel telefoonnummer is 06 13 61 52 25. Waar nodig zullen we additionele gespecialiseerde juridische ondersteuning verkrijgen.

Gerelateerde documenten

Alle documenten relevant voor het uitvoeren van het beleid vind je op Workspace, inclusief de meest recente versie van de projectdocumentatie waarmee het Privacybeleid is opgesteld en vastgesteld op 3 mei 2022 door het MT en de directie.

Woordvoerderschap en communicatie

In alle gevallen zal de directie als woordvoerder optreden bij privacy-gerelateerde voorvallen. We zullen op dat moment handelen naar bevinden, er is geen standaardcommunicatie van toepassing.

Evaluatie en aanpassingen

Dit Privacybeleid en de bijbehorende documenten zullen tweejaarlijks in januari en februari van ieder jaar worden geëvalueerd. Indien nodig zullen er aanpassingen worden gedaan die worden gedeeld met alle direct betrokkenen (medewerkers, MT, Raad van Toezicht). In het Bestuursverslag van de directeur-bestuurder van ieder kalenderjaar wordt uiterlijk eind maart van het betreffende jaar melding gemaakt van:

- Belangrijke incidenten m.b.t. privacy (meldingen, incidenten, voorvallen) voor zover niet reeds eerder tussentijds gedeeld met RvT in het voorgaande jaar, indien zich incidenten hebben voorgedaan
- Grote voorgenomen wijzigingen in het Privacybeleid, indien deze materieel zijn.

Bijlage 1. Verwerkingsregister BLIJ
Bijlage 2. Aanvullende handleiding voor omgang met privacygevoelige gegevens in de Publieksservice
   a. bij dienstverlening aan gebruikers
   b. bij gebruik van BicatWISE
Bijlage 3. Aanvullende handleiding voor omgang met privacygevoelige gegevens in Programma's
   a. van deelnemers aan Programma's.
Bijlage 4. Aanvullende handleiding voor omgang met privacygevoelige gegevens in het Bedrijfsbureau
Bijlage 5. Informatiebeveiligingsbeleid BiSC.
Bijlage 6. Procedure melding datalekken.
Bijlage 7. Meldformulier datalekken BLIJ.

VOORBLAD VERWERKINGSREGISTER

9a. Privacybeleid BLIJ. Bijlage 1. Verwerkingsregister BLIJ 20220502

8-mei-18

					Verwerker	**Systeem**	**Data Inv.**	**Risico-analyse**	**Bijz. data?**	**in de EU?**	**Opt-in Mail**	**GEB?**	**Verw. ovk.**	**Bewaar termijn**	**Wie**	**Contact persoon verw.**	**Status verwerkersovereenkomst**
1	Intern	1	HR	1	Werving en selectie	geen	handmatig	ja	ja	nee	ja	nvt	nvt	nvt	proc.	RH	Gert Staal	nvt
1	Intern	1	HR	2	Personeelsinformatiesysteem	BiSC	AFAS	ja	ja	nee	ja	nvt	nvt	BiSC	5 jaar	RH	Anneke Westland	concept vo gestuurd
1	Intern	1	HR	3	Loonadministratie	BiSC	AFAS	ja	ja	nee	ja	nvt	nvt	BiSC	5 jaar	RH	Anneke Westland	concept vo gestuurd
1	Intern	1	HR	4	Verzuim	CareGroep	VerzuimXpert, AFAS	ja	ja	nee	ja	nvt	nvt	CareGr	5 jaar	RH	Margreet Meijer	vo met softwareleverancier, niet CareGroup
1	Intern	1	HR	5	Vrijwilligersregistratie	geen	geen	ja	ja	nee	ja	nvt	nvt	nvt	5 jaar	RH	Rien Hageman	nvt
1	Intern	1	HR	6	Roosterprogramma	Het Rooster	Het Rooster	ja	ja	nee	ja	nvt	nvt	HR	5 jaar	RH	Godfried Carbo	vo getekend
1	Intern	1	HR	7	Pensioenadministratie	POB	POB	nvt	nvt	nvt	ja	nvt	nvt	nvt	nvt	RH	Rien Hageman	niet noodzakelijk. Email d.d. 8 mei 2018
1	Intern	2	Kantoorautom.	1	Document management in de cloud	Microsoft	Onedrive	ja	ja	nee	ja	nvt	nvt	MS	5 jaar	RH	Rien Hageman	maakt deel uit van licentieovk. MS
1	Intern	2	Kantoorautom.	2	Documentbewerking	BiSC	Microsoft Office	ja	ja	nee	ja	nvt	nvt	BiSC	5 jaar	RH	Anneke Westland	concept vo gestuurd
1	Intern	2	Kantoorautom.	3	Document management, intranet	BiSC	Microsoft	ja	ja	nee	ja	nvt	nvt	BiSC	5 jaar	RH	Anneke Westland	concept vo gestuurd
2	Extern	1	Algemeen	1	CRM	BiSC	Microsoft Dynamics	ja	ja	nee	ja	nvt	nvt	BiSC	5 jaar	RH	Anneke Westland	concept vo gestuurd
2	Extern	1	Algemeen	2	COOSTO	BiSC	COOSTO	ja	ja	nee	ja	nvt	nvt	BiSC	n.b.	RH	Anneke Westland	concept vo gestuurd
2	Extern	1	Algemeen	3	Algemene nieuwsbrief leden	BiSC	HelloDialog	ja	ja	nee	ja	ja	nvt	BiSC	2 jaar	RH	Anneke Westland	concept vo gestuurd
2	Extern	2	Publieksservice	1	Ledenadministratie	BiSC	BicatWISE	ja	ja	nee	ja	nvt	nvt	BiSC	2 jaar	GC	Anneke Westland	concept vo gestuurd
2	Extern	2	Publieksservice	2	Transacties uitleningen	BiSC	BicatWISE	ja	ja	nee	ja	nvt	nvt	BiSC	2 jaar	GC	Anneke Westland	concept vo gestuurd
2	Extern	2	Publieksservice	3	Vrienden-module	BiSC	BicatWISE	ja	ja	nee	ja	nvt	nvt	BiSC	2 jaar	GC	Anneke Westland	concept vo gestuurd
2	Extern	2	Publieksservice	4	Transacties contributies	KB	BicatWISE	ja	ja	nee	ja	nvt	nvt	BiSC	2 jaar	GC	Anneke Westland	concept vo gestuurd
2	Extern	2	Publieksservice	5	Cameraregistratie IJSS	geen	camerasysteem	ja	ja	nee	ja	nvt	nvt	nee	nvt	GC	Godfried Carbo	nvt
2	Extern	2	Publieksservice	6	Bezoekerstellingen	geen	camerasysteem	ja	ja	nee	ja	nvt	nvt	nee	nvt	RH	Rien Hageman	nvt
2	Extern	3	Programma	1	Registratie Taalhuis	Taal vh Leven	Match vh Leven	ja	ja	ja	ja	ja	nvt	nee	2 jaar	AD	Joni Reiche	concept vo gestuurd
2	Extern	3	Programma	2	Registratie DigiSterker	geen	handmatig	ja	ja	ja	ja	ja	nvt	nee	2 jaar	AD	Sabrina Damen	verder inventariseren
2	Extern	3	Programma	3	Registratie VoorleesExpress	geen	handmatig	ja	ja	ja	ja	ja	nvt	nee	2 jaar	AD	Marleen van der Leij	verder inventariseren
2	Extern	3	Programma	4	Educatie-nieuwsbrief 0-6 en 6-12 jr	BiSC	HelloDialog	ja	ja	nee	ja	n.b.	n.b.	BiSC	2 jaar	AD	Anneke Westland	vo getekend
2	Extern	3	Programma	5	Taalhuisnieuwsbrief	geen	MailChimp	ja	ja	nee	nee	nee	n.b.	nvt	2 jaar	AD	Joni Reiche	overstap naar CRM MS Dynamics
2	Extern	3	Programma	6	Nieuwsbrief Uit in IJsselstein	geen	MailChimp	ja	ja	nee	nee	nee	n.b.	nvt	2 jaar	AD	Willeke van Dam	overstap naar CRM MS Dynamics
2	Extern	4	Landelijk	1	Digitale diensten KB voor leden	KB	Bibliotheek.nl	nee	nee	nee	ja	in afwa	nee	waarsc	2 jaar	n.b.	Naomi Deegenaars	vo getekend

Bijlage 2. Aanvullende handleiding Publieksservice

a. Handleiding voor omgang met persoonsgegevens in BicatWISE in de Publieksservice

Aanvullende handleidingen voor Publieksservice: verwerken van persoonsgegevens in BicatWISE

1. Locatie van en toegang tot bestanden en systemen
- Inlognamen en wachtwoorden (persoonlijke inlog)
- Beheer inlognamen en wachtwoorden
2. Invoer van persoonsgegevens (leden)
- Melden van opslag persoonsgegevens aan nieuw lid bij inschrijving
- Toestemming voor toezending van:
    - Informatie betreffende lidmaatschap
    - Informatie over evenementen in de bibliotheek (nieuwsbrieven)
    - Wervende informatie
- Toestemming voor gebruik gegevens door derden kan soms nodig zijn. We kunnen dit opnemen in het reglement.
- Welke gegevens worden bewaard? Persoonsgegevens, financiële gegevens en uitleentransacties (leenhistorie)
3. Mutaties van het lidmaatschap
- Wanneer vinden er mutaties plaats?
    - Als een klant zich inschrijft of opzegt,
    - Als een klant van abonnement verandert
    - Als een klant de jaarlijkse contributie, openstaande boetes of bijdragen betaalt
    - Als een klant in aanmerking komt voor kortingen op het abonnement
- Wie mag ze doorvoeren?
    - Medewerkers en vrijwilligers schrijven klanten in
    - De ledenadministratie is verantwoordelijk voor de afhandeling van opzeggingen en de contributiebetalingen.
    - Medewerkers/vrijwilligers in de PS handelen kortingen, boetes en bijdragen af en mutaties in abonnementsvorm
4. Doorgeven van persoonsgegevens aan subsidiënten: De bibliotheek geeft NOOIT gegevens af die op de persoon zijn te herleiden aan een subsidiënt. Subsidiënten ontvangen rapportages op basis van aantallen leden, aantallen uitleningen, of geanonimiseerde bestanden.
5. Beëindiging lidmaatschap:
- Hoe lang wordt informatie bewaard in BicatWISE?
- Wie wist de persoonsgegevens? De BISC, als beheerder, kan als enige binnen het systeem de persoonsgegevens volledig verwijderen
- Wanneer schonen wij bestanden op? Dat gebeurt ieder jaar in januari en februari.
- Hoe vindt het wissen plaats? Handmatig. Binnen systemen wel batch-gewijs.

b. Handleiding voor omgang met privacy-gevoelige gegevens van klanten in de Publieksservice

Inleiding

In 2018 is de nieuwe AVG wetgeving van kracht geworden op het gebied van persoonsgegevens, die de oude regelingen vervangt. Als bibliotheek moeten wij werken aan de bewustwording van alle medewerkers en vrijwilligers op het gebied van het verwerken van persoonsgegevens en regels rondom privacy.

Bibliotheken spelen een actieve rol in het sociale domein en breiden hun dienstverlening steeds meer uit. Denk dan bijvoorbeeld aan het convenant dat in 2016 met de Belastingdienst is afgesloten. De medewerkers en vrijwilligers in de publieksservice worden daardoor steeds vaker geconfronteerd met hulpvragen waarbij privacyaspecten en gevoelige financiële informatie een rol spelen. Het is belangrijk dat wij als Bibliotheek hier goed op zijn voorbereid en met set afspraken de medewerkers in de publieksservice ondersteunen. Zo hoeven medewerkers niet zelf te bepalen hoe ver ze gaan in het helpen van de klant en vermijdt de Bibliotheek onnodige risico's.

Om de medewerker goed toe te rusten, moet de Bibliotheek een aantal randvoorwaarden realiseren. Dit document is bedoeld als kader voor de afspraken, uitgangspunten, gedragsregels en voorbeeldsituaties. Dit kader is niet bedoeld voor de dagelijkse praktijk. Het is een naslagwerk en dient als uitgangspunt voor de bewustwording van de medewerkers. Voor de dagelijkse praktijk is een verkort overzicht van afspraken opgesteld per locatie, met daarin de belangrijkste punten op een rij. Deze uitgebreide handleiding en de verkorte versies zijn opgenomen in het Handboek PS

De bibliotheekrealiteit zal door maatschappelijke en technische ontwikkelingen blijven veranderen. Dit is daarom geen statisch document. Het wordt waar nodig aangepast en is afhankelijk van de situatie.

Afspraken t.a.v. klantcontact met privacygevoelige, juridische en financiële informatie

Waar gaat deze afspraken over

De afspraken helpen je omgaan met ad hoc vragen met privacygevoelige, juridische en financiële informatie. Wat zegt de wetgever? Wat na de invoering van de AVG nog wel en niet meer doen? Waar help je wel mee en waarmee niet? Hoe ver ga je?

Waar gaat deze afspraken niet over

De afspraken gaat niet over klantcontacten waarin privacygevoelige en financiële handelingen geen rol spelen. Dat is het gros van de klantcontacten.

Voorbeeldsituaties

- Een klant komt naar je toe en vraagt jouw hulp bij handelingen op de computer waarbij persoonlijke en/of financiële gegevens op het beeldscherm verschijnen.
- In de Bibliotheek verricht een klant financiële handelingen op de computer (internetbankieren, (belasting)zaken et cetera) of zaken waarbij persoonlijke gegevens in beeld komen (werkdossier UWV, Facebook, chatten, mailen et cetera). De klant komt er niet uit en vraagt jouw hulp.

- Je helpt een klant aan de balie en zoekt zijn gegevens op in het bibliotheeksysteem. Kort daarop moet jij de personeelspc verlaten om werkzaamheden elders te doen.
- Een klant kopieert een document en laat het origineel liggen.
- Een klant heeft problemen met de apparatuur of digitale diensten van de Bibliotheek (bijvoorbeeld het e-books aanbod, de Vakantiebieb, Mijn Bibliotheek, Mijn Menu, et cetera). Tijdens de reguliere uitlening.

Een klant heeft problemen met de apparatuur of digitale diensten van de Bibliotheek (bijvoorbeeld het e-book-aanbod, de Vakantiebieb, Mijn Bibliotheek, et cetera). Dat kan zijn tijdens een spreekuur. Dit zijn slechts voorbeelden van veelvoorkomende situaties. Je kunt ook andere vragen krijgen waarin privacy en persoonlijke financiën een rol spelen.

Uitgangspunt van de Bibliotheek

De Bibliotheek speelt een actieve rol in het publieke en sociale domein. Dit doet zij door een laagdrempelige, voor iedereen toegankelijke plaats te bieden om anderen te ontmoeten, te lezen, te leren, je te ontwikkelen en wijzer te worden.

De Bibliotheek ondersteunt mensen om *zelfredzaam* te worden en blijven. De Bibliotheek ontleent haar maatschappelijke betekenis aan de mate waarin burgers, mede dankzij de Bibliotheek, meer grip op hun leven kunnen hebben.

De bibliotheekmedewerker is zelf geen inhoudelijk specialist, maar weet hoe hij of zij de vraag analyseert, informatie zoekt en de klant doorverwijst. De medewerker is tussenpersoon tussen klantvraag en informatie.

Niveau van de dienstverlening

Je laat zien waar de klant de informatie kan vinden, en (als dat relevant is) waar en hoe hij iets kan doen (bijvoorbeeld inloggen)

- Je laat de klant inloggen
- Je kijkt niet mee als de klant inlogt
- Je helpt de klant na het inloggen, maar je voert geen handelingen uit.
- Je coacht en legt uit
- Je laat de klant *zelf* alle handelingen uitvoeren, tenzij de klant uitdrukkelijk assistentie zou vragen (zie beneden).

Je legt de klant uit waarom je op deze manier helpt, maakt hem bewust van de risico's en verwijst – indien nodig – door naar andere instanties of een apart aanbod van de Bibliotheek (spreekuur, cursus et cetera).

Uitzondering

Bij een technisch probleem van de bibliotheekapparatuur, als de klant het digitale spreekuur bezoekt of als het een product van de Bibliotheek betreft, geldt een uitzondering. Denk hierbij aan e-books, e-readers, de apps, de website van de Bibliotheek, mijn bibliotheek-omgeving, et cetera. Dan help je de klant – *als dat nodig is* – door de muis, of de besturing van de tablet, smartphone of tablet over te nemen. Je voert dan handelingen uit voor de klant. Voordat je dat doet, vraag je de klant om toestemming en maak je hem bewust van de risico's. Alle informatie over deze gebruiker benodigd voor de hulpvraag zoals inloggegevens of persoonlijke gegevens wordt direct na het contact vernietigd (papier of digitale gegevens).

Algemeen

Wat vraag je

- Je probeert duidelijk te krijgen waarbij de klant precies hulp nodig heeft en vraagt door.
- Je probeert vooraf vast te stellen of je de klant zelf kunt helpen of dat je kunt doorverwijzen naar een andere organisatie of een cursus of spreekuur in de Bibliotheek.
- Je informeert naar de urgentie van de vraag. Dit helpt bij het bepalen van de beste oplossing.

- Als een klant je hulp vraagt terwijl hij al achter de computer zit, vraag dan altijd of er privacygevoelige informatie op het scherm staat. Het is niet de bedoeling dat je die ziet, zonder dat de klant daarvoor toestemming heeft gegeven.

Wat vertel je

- Als je vraagt of er privacygevoelige informatie op het scherm staat en het antwoord is positief, vraag dan uitdrukkelijk toestemming om mee te kijken.
- Maak de klant bewust van de risico's die hij neemt als hij anderen in vertrouwen neemt en gevoelige handelingen uitvoert op de computers en via het netwerk van de Bibliotheek.
- Maak de klant duidelijk dat het ten zeerste af te raden is om financiële en andere transacties met persoonlijke gegevens te verrichten via de wifi-verbinding van de Bibliotheek. Het veiligste doet de klant dit op zijn smartphone (of tablet) via het mobiele netwerk (3G en 4G) via de app van de bank.

“Staat er privacygevoelige informatie op uw scherm? Als ik u help kan ik deze informatie zien. Heeft u daar bezwaar tegen? Ik zal er uiterst vertrouwelijk me omgaan.”

“Ik wil u graag helpen met de techniek, maar ik kan u geen financieel advies geven. In de Bibliotheek hebben wij onvoldoende kennis om u inhoudelijk met deze vraag te helpen”
“Ik kan u wel een adres geven waar u met uw vraag geholpen kunt worden.”

“Vindt u het lastig om om te gaan met de digitale wereld? Wij hebben cursussen die u daarbij helpen!
Vraag naar onze cursussen 'Klik & Tik' en 'Omgaan met de e-overheid'. Deze cursussen bieden bij gratis aan."

Bij uitzondering tijdens het digitale spreekuur mag je de besturing overnemen en handelingen voor de klant uitvoeren:
“Heeft u er bezwaar tegen dat ik met u meekijk? Het kan zijn dat ik persoonlijke gegevens zie, maar die zal ik in vertrouwen behandelen”
“Ik log niet voor u in.”
“Heeft er bezwaar tegen dat ik de muis overneem?”

Wat is je houding?

- Je bent klantvriendelijk en open.
- Je bent servicegericht, hebt dienstverlening hoog in het vaandel staan
- Je bent duidelijk en geeft de grenzen aan.
- Je weet dat “Nee” ook een antwoord is, maar je legt wel uit waarom en biedt alternatieven.
- Je bent begripvol, maar laat je niet leiden door de (morele) druk die de klant je oplegt.
- Je zorgt dat je het probleem van de klant niet het jouwe maakt.
- De klant is eindverantwoordelijk voor zijn handelingen en beslissingen.
- Je schiet niet meteen in de hulphouding, maar informeert waar het voor is en hoe urgent de vraag is.
- Je verwijst door naar eigen diensten (spreekuur, cursus) of naar organisaties in de regio.
- Je focust je op de zelfredzaamheid van de klant. Zorg dat helpen geen kortstondig succes is, want dan staat de klant morgen weer voor je balie met dezelfde vraag.
- Je houdt persoonlijke gegevens van de klant geheim.
- Je gaat vertrouwelijk om met de privacygevoelige vragen van klanten.
- Je geeft geen financieel advies. Daar ligt niet de deskundigheid van de bibliotheek. Het geven van advies leidt juridisch gezien tot een “overeenkomst van opdracht”. Daarbij heeft de bibliotheek als opdrachtnemer een zorgplicht. De bibliotheek is dus medeverantwoordelijk voor het advies en de daaruit voortvloeiende consequenties. De bibliotheek moet nazorg kunnen verlenen. Adviseren over bijvoorbeeld belastingen en internetbankieren is dus (zeer) risicovol.
- Je blijft kritisch. Denk na voordat je handelt. Stel jezelf de vraag: “hoe zou ik het vinden als het om mijn gegevens zou gaan.”

Wat doe je wel

- Je laat de klant zien waar hij de informatie kan vinden.

- Je laat zien waar de klant dient in te loggen.
- Je kijkt niet mee als de klant inlogt.
- Alleen als het écht nodig is kijk je mee met de klant nadat hij heeft ingelogd.
- Je vergrendelt de computer als je wegloopt bij de personeelsterminal (Windowstoets + L, of de combinatie CTRL-ALT-DEL.

Bij bibliotheekdiensten en –producten, tijdens het digitale spreekuur geldt een uitzondering

- Tijdens het digitale spreekuur mag je de bediening van de computer, tablet, smartphone, e-reader (…) van de klant overnemen. Ook na het inloggen. Let wel als het echt niet anders gaat én het om een dienst/product van de bibliotheek gaat.

Wat doe je niet

- Je logt niet in voor de klant.
- Je neemt de muis niet over.
- Je voert geen handelingen voor de klant uit.
- Je geeft geen financieel advies.
- Je laat geen gegevens op een personeelsterminal staan als je wegloopt.
- Je gaat er niet van uit dat iemand toestemming zal geven. Je vraagt altijd om toestemming om mee te kijken.

Bij bibliotheekdiensten en -producten geldt een uitzondering

- Je gaat er niet zomaar van uit dat iemand toestemming zal geven. Je vraagt altijd om toestemming om mee te kijken en de bediening over te nemen.
- Je logt niet in voor de klant. Je hebt niets te maken met de inloggegevens van de klant.

Wat als je er niet zelf uitkomt?

Neem voor vragen contact op met jouw leidinggevende, of als het om Digisterker/Taalhuis met je Medewerker Projecten of Projectleider.

Techniek

Publiekspc's

- Als de klant gebruikmaakt van de publiekspc's laat hij digitale sporen na, zoals:
  - Bezochte websites
  - Verstuurde mails
  - Geopende en/of gedeelde en foto's en video's
  - Opgeslagen en/of geprinte bestanden die je deelt
- Alle bestanden (Office, afbeeldingen, pdf) blijven staan tot de Bibliotheek sluit: dan worden alle persoonlijke gegevens van de klanten van het systeem gewist.
- De schermen van de publiekspc's zijn met opzet voor iedereen zichtbaar. We willen zo toezicht houden op hoe de pc's gebruikt worden en kunnen ingrijpen als er bijvoorbeeld porno, geweld of andere ongewenste informatie in de Bibliotheek wordt bekeken.
- De schermen van de publiekspc's zijn met opzet voor iedereen zichtbaar. Daarmee moeten gebruikers dus rekening houden wanneer zij persoonlijke en/of gevoelige informatie op het scherm hebben.

Printen en scannen

- De printers en scanners zijn voor iedereen toegankelijk.
- Om te printen geeft de klant een printopdracht vanaf de publiekspc. De klant moet voor printen en kopiëren een tegoed kopen bij de betaalautomaat. Procedure hangt bij het apparaat.
- De klant dient zelf de print op te halen.
- Soms blijven documenten liggen bij de printer, scanner of kopieerapparaat. Als het om privacygevoelige informatie gaat neemt de medewerker deze mee een geeft deze aan de coördinator publieksservice. Is de eigenaar van de documenten niet te vinden en worden de documenten niet binnen een week opgehaald,

lever ze dan in overleg met de coördinator publieksservice af bij het politiebureau als het gaat om officiële documenten of het loket gevonden voorwerpen. Zijn het geen officiële documenten, vernietig ze dan.

Wifi

- De Bibliotheek biedt open en gratis wifi aan. Het wachtwoord hiervan is publiekelijk bekend (Lekijssel).
- Het gebruik van een open wifi-verbinding is per definitie niet veilig. Kwaadwillenden kunnen vrij simpel met de juiste apparatuur de wifi-verbinding afluisteren en alle verstuurde gegevens opslaan, inclusief wachtwoorden en andere persoonlijke gegevens. Deze gegevens kunnen zij vervolgens gebruiken om identiteitsfraude mee te plegen. Om die reden maakt de belasting-pc gebruik van een vaste verbinding.
- Financiële transacties verrichten via de wifi-verbinding van de Bibliotheek is ten zeerste af te raden. Het veiligste doet de klant dit op zijn smartphone (of tablet) via het mobiele netwerk (3G en 4G) via de app van de bank.

.

Handige snelkoppelingen in verband met privacy

Windows

Ctrl + P	=	Printen/afdrukken
Windows-toets + L	=	Computer vergrendelen
Windows-toets + D	=	Alle openstaande schermen minimaliseren

Wise

F12	=	Klant afsluiten

Doorverwijzen

- De Medewerker Projecten onderhoudt een actueel overzicht met doorverwijsadressen. Daarin staat ook het overzicht van wat deze instanties aan diensten kunnen bieden.
- De Bibliotheek organiseert diverse cursussen, zoals Klik & Tik en Werken met de e-Overheid van Digisterker. Van deze cursussen zijn folders e.d. gemaakt. Informatie is te vinden op de website van het Taalhuis. Voor complexe vragen zijn er inloopspreekuren in de Bibliotheek waar klanten uitgebreider geholpen worden.

Situaties

Een klant komt naar je toe en vraagt jouw hulp bij handelingen op de computer waarbij persoonlijke en/of financiële gegevens op het beeldscherm verschijnen.

Weet

- Dat het niet gewenst is dat jij als medewerker meekijkt met de klant als er privacygevoelige en financiële gegevens op het scherm staan.
- Dat het echter soms niet te vermijden is dat je meekijkt nadat de klant al is ingelogd.
- Dat je daar nadrukkelijk toestemming voor vraagt.
- Dat je geen handelingen voor de klant uitvoert en dat het niet de bedoeling is dat je meekijkt met het inloggen.
- Dat de collega's van het digitale spreekuur een stap verder mogen gaan.
- Dat het risicovol is om klanten te helpen met privacygevoelige en financiële vragen. Het kan voor de klant nadelige gevolgen hebben en tot misverstanden leiden. Dat hoeft niet de schuld van de bibliotheekmedewerker te zijn, maar dat realiseert de klant zich vaak niet. En dat kan leiden tot verwijten, claims en imagoschade.
- Dat het helpen van klanten vaak een kortstondig succes is, maar het aanleren van handelingen effectiever is. Zo maak je de klant zelfredzaam.

- Dat er veiligheidsrisico's zijn verbonden aan financiële transacties verrichten via openbare computers en openbaar wifi.
- Dat de klant is geholpen met een duidelijk verhaal en goede alternatieven.

Verhaal
- Je schiet niet meteen in de hulphouding, maar informeert waar het voor is en hoe urgent de vraag is.
- Je geeft aan dat je als medewerker van de Bibliotheek de klant kunt helpen, maar dat je niet meekijkt met het inloggen. Die gegevens zijn vertrouwelijk en daar heb jij (en anderen) niets mee te maken. Zodra de klant is ingelogd ben je bereid om - als het niet anders kan - mee te kijken. Datgene wat je ziet zal je vertrouwelijk behandelen.

Doen
- Je vraagt door en bepaalt de urgentie.
- Je laat de klant zien waar hij de informatie kan vinden.
- Je laat zien waar de klant dient in te loggen.
- Je kijkt bewust en zichtbaar weg van het scherm zodra de klant gaat inloggen.
- Je helpt – als het niet anders kan – verder nadat de klant is ingelogd.
- Je verwijst indien nodig door naar een andere organisatie, of naar een cursus of spreekuur in de Bibliotheek.

Laten
- Je logt niet in voor de klant.
- Je kijkt niet mee als de klant inlogt.
- Je neemt de muis niet over.
- Je voert geen handelingen voor de klant uit.
- Je geeft geen financieel advies.
- Je gaat er niet voetstoots van uit dat iemand toestemming zal geven.

In de Bibliotheek verricht een klant financiële handelingen op de computer (internetbankieren, (belasting)zaken et cetera) of zaken waarbij persoonlijke gegevens in beeld komen (werkdossier UWV, Facebook, chatten, mailen et cetera). De klant vraagt jouw hulp.

Weet
- Dat het niet gewenst is dat jij als medewerker meekijkt met de klant als er privacygevoelige en financiële gegevens op het scherm staan.
- Dat je dat altijd moet checken, alvorens je de klant gaat helpen.
- Dat het echter soms niet te vermijden is dat je meekijkt nadat de klant al is ingelogd.
- Dat je daar nadrukkelijk toestemming voor vraagt.
- Dat je geen handelingen voor de klant uitvoert en dat het niet de bedoeling is dat je meekijkt met het inloggen.
- Dat de collega's van het digitale spreekuur een stap verder mogen gaan.
- Dat het risicovol is om klanten te helpen met privacygevoelige en financiële vragen. Het kan voor de klant nadelige gevolgen hebben en tot misverstanden leiden. Dat hoeft niet de schuld van de bibliotheekmedewerker te zijn, maar dat realiseert de klant zich vaak niet. En dat kan leiden tot verwijten, claims en imagoschade.
- Dat het helpen van klanten vaak een kortstondig succes is, maar het aanleren van handelingen effectiever is. Zo maak je de klant zelfredzaam.
- Dat er veiligheidsrisico's zijn verbonden aan financiële transacties verrichten via openbare computers en openbaar wifi.
- Dat de klant is geholpen met een duidelijk verhaal en goede alternatieven.

Verhaal
- Je schiet niet meteen in de hulphouding, maar informeert waar het voor is en hoe urgent de vraag is.
- Je geeft aan dat je als medewerker van de Bibliotheek de klant kunt helpen, maar dat je niet meekijkt met het inloggen. Die gegevens zijn vertrouwelijk en daar heb jij (en anderen) niets mee te maken. Zodra de klant is ingelogd ben je bereid om - als het niet anders kan - mee te kijken. Datgene wat je ziet zal je vertrouwelijk behandelen.

Doen
- Je informeert altijd of er persoonlijke of financiële gegevens op het beeldscherm staan. Het is niet de bedoeling dat jij die ziet.
- Je vraagt door en bepaalt de urgentie.
- Je laat de klant zien waar hij de informatie kan vinden.
- Je laat zien waar de klant dient in te loggen.
- Je kijkt bewust en zichtbaar weg van het scherm zodra de klant gaat inloggen.
- Je helpt – als het niet anders kan – verder nadat de klant is ingelogd.
- Je verwijst indien nodig door naar een andere organisatie, of naar een cursus of spreekuur in de Bibliotheek.

Laten
- Je logt niet in voor de klant.
- Je kijkt niet mee als de klant inlogt.
- Je neemt de muis niet over.
- Je voert geen handelingen voor de klant uit.
- Je geeft geen financieel advies.
- Je gaat er niet voetstoots van uit dat iemand toestemming zal geven.

Je helpt een klant aan de balie en zoekt zijn gegevens op in het Bibliotheeksysteem. Kort daarop moet jij de personeelspc verlaten om werkzaamheden elders te doen.

Weet
- Dat alle dienstverlening in de publieksservice vertrouwelijke of persoonsgegevens kan betreffen.
- Dat klanten de gegevens van andere klanten niet mogen zien.
- Dat klanten geen handelingen mogen verrichten op de personeelspc's.
- Dat je geen documenten mag openen voor klanten op de personeelspc's i.v.m. het gevaar op virus- en malwarebesmetting.

Doen
- Je sluit het scherm altijd af als je wegloopt. (Windowstoets + L)
- Je sluit in Wise altijd de klant af (F12).
- Je minimaliseert het mailprogramma.
- Je denkt om je stemvolume in een gesprek over privacygevoelige informatie met een klant of een collega. Desnoods doe je dat in een andere ruimte.

Laten
- Je laat geen briefjes slingeren met klantgegevens.
- Je stopt geen USB-sticks van klanten in de personeelspc.
- Je opent geen documenten van klanten op de personeelspc.

Een klant kopieert of scant een document en laat het origineel liggen.

Doen

- Je kijkt in Wise of de documenten van een klant zijn.
- Je probeert het telefoonnummer of mailadres te achterhalen van de eigenaar.
- Je waarschuwt de eigenaar en verzoekt de documenten binnen een week af te halen of spreekt een langere periode af.
- Je stopt de documenten in een envelop, met de naam van de eigenaar en de datum dat het document gevonden is en eventueel de datum van afhalen.
- Je bewaart de envelop op een vaste afgesloten plek.
- Als je de eigenaar niet kunt achterhalen, dan wordt een document ten minste één week bewaard.
- Is de eigenaar van de documenten niet gevonden en worden de documenten niet binnen een week opgehaald, lever ze dan in overleg met de publieksservice-coördinator af bij het politiebureau of loket gevonden voorwerpen. Zijn het geen officiële documenten, vernietig ze dan.

Laten

- Je laat de documenten niet liggen.
- Je laat de documenten niet in het zicht op de balie liggen.

Een klant heeft problemen met de apparatuur of digitale diensten van de Bibliotheek (bijvoorbeeld het e-bookaanbod, de Vakantiebieb, Mijn Bibliotheek, et cetera). Tijdens de reguliere uitlening.

Het verschil met deze werkwijze en die van het digitale spreekuur is gelegen in de tijd en de deskundigheid die jij als publieksservicemedewerker hebt. Kost het helpen te veel tijd en/of je hebt niet voldoende kennis, verwijs dan door naar het digitale spreekuur.

Weet

- Dat het bij uitzondering toegestaan is dat jij als medewerker meekijkt met de klant nadat deze heeft ingelogd.
- Dat het bij uitzondering toegestaan is dat jij als medewerker de besturing van de computer/tablet/smartphone/e-reader/… van de klant overneemt.
- Deze uitzondering geldt alleen als het gaat om producten van de bibliotheek.
- Dat je klanten alleen helpt als daar qua tijd voldoende ruimte voor is. Zo niet dan verwijs je door naar het digitale spreekuur.

Verhaal

- Je vraagt uitdrukkelijk toestemming om mee te kijken met de klant.
- Je vraagt uitdrukkelijk toestemming voordat je de besturing overneemt van de computer/tablet/smartphone/e-reader/… van de klant.
- Je schiet niet meteen in de hulphouding, maar informeert waar het voor is en hoe urgent de vraag is.
- Neemt de vraag veel tijd in beslag of is jouw kennis onvoldoende, verwijs de klant dan door naar het digitale spreekuur van de Bibliotheek.

Doen

- Je vraagt door en bepaalt de urgentie.
- Je laat de klant zien waar hij de informatie kan vinden.
- Je laat zien waar de klant dient in te loggen.
- Je kijkt bewust en zichtbaar weg van het scherm zodra de klant gaat inloggen.
- Je helpt – als het niet anders kan – verder nadat de klant is ingelogd.
- Je vraagt uitdrukkelijk toestemming om mee te kijken met de klant en de besturing van zijn apparaat over te nemen.
- Je verwijst indien nodig door naar een andere organisatie, of naar een cursus of spreekuur in de Bibliotheek.

Laten

- Je logt niet in voor de klant.
- Je kijkt niet mee als de klant inlogt.
- Je geeft geen financieel advies.
- Je gaat er niet voetstoots van uit dat iemand toestemming zal geven.

Een klant heeft problemen met de apparatuur of digitale diensten van de Bibliotheek (bijvoorbeeld het e-bookaanbod, de Vakantiebieb, Mijn Bibliotheek, et cetera). Tijdens een spreekuur.

Het verschil met deze werkwijze en die van de publieksservice is gelegen in de tijd en de deskundigheid die jij als publieksservicemedewerker hebt. Tijdens het spreekuur is er meer tijd en heb jij als medewerker meer kennis van de materie.

Weet

- Dat het bij uitzondering toegestaan is dat jij als medewerker meekijkt met de klant nadat deze heeft ingelogd.
- Dat het bij uitzondering toegestaan is dat jij als medewerker de besturing van de computer/tablet/smartphone/e-reader/… van de klant overneemt.
- Deze uitzondering geldt alleen als het gaat om producten van de bibliotheek.

Verhaal

- Je vraagt uitdrukkelijk toestemming om mee te kijken met de klant.
- Je vraagt uitdrukkelijk toestemming voordat je de besturing overneemt van de computer/tablet/smartphone/e-reader/… van de klant.
- Je schiet niet meteen in de hulphouding, maar informeert waar het voor is.

Doen

- Je vraagt door en bepaalt de urgentie.
- Je laat de klant zien waar hij de informatie kan vinden.
- Je laat zien waar de klant dient in te loggen.
- Je kijkt bewust en zichtbaar weg van het scherm zodra de klant gaat inloggen.
- Je helpt – als het niet anders kan – verder nadat de klant is ingelogd. Je mag daarbij meekijken en de besturing overnemen van de computer/tablet/smartphone/e-reader/… van de klant.
- Je vraagt uitdrukkelijk toestemming om mee te kijken met de klant en de besturing van zijn apparaat over te nemen.
- Je verwijst indien nodig door naar een andere organisatie, of naar een cursus in de Bibliotheek.

Laten

- Je logt niet in voor de klant.
- Je kijkt niet mee als de klant inlogt.
- Je geeft geen financieel advies.
- Je gaat er niet voetstoots van uit dat iemand toestemming zal geven.

Bijlage 3. Aanvullende handleiding Programma's

Dit onderdeel betreft aanwijzingen voor het verwerken persoonsgegevens voor alle activiteiten uitgevoerd door de afdeling Programma's (Sociaal Domein en Educatie).

1. Locatie van en toegang tot bestanden en systemen:
- Evt. inlognamen en wachtwoorden v.z.v. geen handmatige verwerking
- Beheer inlognamen en wachtwoorden
2. Invoer van persoonsgegevens (leden):
- Melden van opslag persoonsgegevens aan nieuwe deelnemer
- Toestemming voor toezending van:
    - Informatie betreffende lidmaatschap
    - Informatie over evenementen in de bibliotheek
    - Wervende informatie?
- Toestemming voor gebruik gegevens door derden indien van toepassing (bijv. UWV)
- Welke gegevens worden bewaard? *Welke mogen niet worden bewaard?*
3. Mutaties deelnemers:
- Wanneer vinden er mutaties plaats?
- Wie mag ze doorvoeren?
4. Doorgeven van persoonsgegevens aan subsidiënten: alleen geaggregeerd voor rapportagedoeleinden, NOOIT op persoon
5. Beëindiging deelname aan programmaonderdeel:
- Hoe lang wordt informatie bewaard?
- Wie wist de persoonsgegevens?
- Wanneer schonen wij bestanden op?
- Hoe vindt wissen plaats?

Aanvullingen voor de VoorleesExpress

Privacy van onze vrijwilligers en gezinnen is een belangrijk thema waar we veel aandacht aan besteden. Dat geldt voor Mijn VoorleesExpress, maar ook daarbuiten.

Wij zorgen ervoor dat technisch aan alle eisen wordt voldaan. Werken met Mijn VoorleesExpress betekent dat een aantal zaken al goed geregeld zijn. Alle beheerders van een eigen omgeving tekenen een verwerkersovereenkomst met Stichting VoorleesExpress waarin staat wie waar verantwoordelijk voor is.

Belangrijke aandachtspunten:

- Goed omgaan met wachtwoorden. Je Mijn VoorleesExpress wachtwoord regelmatig wijzigen. Zorgen dat computers beveiligd zijn met een wachtwoord en ervoor zorgen dat je wachtwoord niet onthouden wordt in de browser. Dit zijn zaken die wij niet kunnen regelen, die moeten jullie lokaal borgen.
- Gebruik geen andere intake formulieren dan het aanmeldformulier in Mijn VoorleesExpress. Wat je wel en niet mag opslaan luistert nogal nauw. Wij zorgen ervoor dat er in Mijn VoorleesExpress alleen vragen gesteld worden die passen binnen de wetgeving. Wees er als projectleider waakzaam op wat je toeleiders en vrijwilligers allemaal toevoegen. Laat ze enkel informatie schrijven die relevant is voor het project en die je het gezin zelf ook zou vertellen. Gezinnen mogen ten alle tijden inzien wat er over ze geschreven staat.

Wat mag niet?

Bijzondere persoonsgegevens opslaan. Onder bijzondere of gevoelige persoonsgegevens vallen:

- gegevens die iets zeggen over iemands ras (en hieraan gelinkt afkomst of moedertaal)
- gegevens over godsdienst
- gegevens over gezondheid
- strafrechtelijk verleden
- geslacht, gender, seksuele voorkeuren, seksleven.
- gegevens opslaan die niet nodig zijn voor de uitvoer van de VoorleesExpress (denk aan verslaglegging die vrijwilligers doen over situaties thuis die niets te maken hebben met het doel van de VoorleesExpress)
- Ook het burgerservicenummer (BSN) valt onder de bijzondere persoonsgegevens (je mag dus ook geen kopie maken van een ID of paspoort).

In beginsel mag je alleen opslaan wat voor de activiteit in kwestie noodzakelijk en relevant is.

Wat mag wel?

Informatie opslaan die onmisbaar is voor de uitvoer van de VoorleesExpress als gebruikers hier toestemming voor geven. Toestemming geven ze op moment van aanmelding via Mijn VoorleesExpress. Wanneer je als projectleider zelf aanmeldingen overneemt dan sla je die stap over.

Inzage recht

Alle gebruikers hebben het recht om hun eigen gegevens in te zien, te (laten) wijzigen of verwijderen.

Lijst met afgewezen voorlezers

Een belangrijk aandachtspunt is de lijst met afgewezen voorlezers. Deze lijst mag je niet delen buiten je organisatie, hij is enkel voor intern gebruik i.v.m. de veiligheid van onze deelnemers.

Bijlage 4. Aanvullende handleiding Bedrijfsbureau

Verwerken van persoonsgegevens van werknemers en vrijwilligers (meer specifiek AFAS en bijv. VerzuimXpert).

1. Locatie van en toegang tot bestanden en systemen:
- Evt. inlognamen en wachtwoorden v.z.v. geen handmatige verwerking
- Beheer inlognamen en wachtwoorden
2. Invoer van persoonsgegevens werknemers en vrijwilligers:
- Melden van opslag persoonsgegevens aan nieuwe werknemer of vrijwilliger
- Toestemming voor toezending van:
    - Informatie betreffende arbeidsverband
    - Informatie over evenementen voor werknemers en/of vrijwilligers
- Toestemming voor gebruik gegevens door derden indien van toepassing (bijv. UWV, Belastingdienst)
- Welke gegevens worden bewaard? *Welke mogen niet worden bewaard?*
3. Mutaties werknemers en vrijwilligers:
- Wanneer vinden er mutaties plaats?
- Wie mag ze doorvoeren?
4. Doorgeven van persoonsgegevens aan UWV en Belastingdienst?
5. Beëindiging arbeidsrelatie:
- Hoe lang wordt informatie bewaard?
- Wie wist de persoonsgegevens?
- Wanneer schonen wij bestanden op?
- Hoe vindt het wissen plaats?

Procedure melding datalekken

Algemeen

Ingangsdatum:	25 mei 2018
Wijzigingsdatum:	3 mei 2022
Versie:	1.1
Opgesteld door:	Gert Staal, directeur-bestuurder
Vastgesteld op:	3 mei 2022 door MT en directie
Ondertekening:	Gert Staal, 3 mei 2022

Inleiding

Dit document geeft een beschrijving van verschillende rollen en fases omtrent de afhandeling van beveiligingsincidenten en datalekken.

Standaardprocedure meldplicht datalekken

Het proces gaat uit van drie rollen en zes fases. Een belangrijk uitgangspunt is dat het proces ertoe moet leiden dat alle relevante feiten goed worden vastgelegd gedurende de afwikkeling van een beveiligingsincident/mogelijk datalek. Voor het vastleggen van deze feiten bevat de Toolkit het document 12b. Meldplicht datalekken: sjabloon.

Beveiligingsincident of datalek?

Een datalek is een beveiligingsincident waarbij persoonsgegevens verloren zijn gegaan, waarbij de persoonsgegevens onrechtmatig verwerkt zijn of wanneer het niet redelijkerwijs uitgesloten kan één van deze mogelijkheden plaats heeft gevonden. Indien dit niet het geval is, is het dus een beveiligingsincident. Wanneer de organisatie tot de conclusie komt dat het om een datalek gaat, moet worden bepaald of er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens. Afhankelijk daarvan moet het datalek gemeld worden aan de Autoriteit Persoonsgegevens (hierna: AP), of niet.

Standaardprocedure meldplicht datalekken: rolverdeling

Om de juiste informatie tijdig op de juiste plek te krijgen, is het van belang om de voor de afhandeling van een beveiligingsincident en dus een mogelijk datalek, de relevante rollen en verantwoordelijkheden vast te stellen. De proceseigenaar is de manager bedrijfsvoering.

Wij onderscheiden drie rollen:

Rol	*Uitleg*	*Voorbeeld*
Ontdekker	Degene die het beveiligingsincident en mogelijk datalek op het spoor komt, vaak ook degene die (in eerste instantie) over de meeste informatie beschikt.	Frontoffice-medewerker, lid webcareteam, systeembeheerder etc.
Technicus	Degene die, indien het datalek een technische oorzaak heeft (wat vaak het geval zal zijn), maatregelen kan nemen zodat het lek 'gedicht' wordt.	Systeembeheerder BiSC
Melder	Degene die belast is met het vergaren van de relevante informatie om op basis daarvan een melding te kunnen doen aan de AP en eventueel aan getroffen klanten.	Manager bedrijfsvoering

De hierboven beschreven rollen hebben ieder hun eigen verantwoordelijkheden. Hierna worden deze kort omschreven.

Ontdekker

De ontdekker is degene die een beveiligingsincident/mogelijk datalek signaleert en daarover rapporteert bij de melder binnen organisatie waarvoor hij of zij werkzaam is. Omdat de ontdekker aanvankelijk het dichtst op het mogelijke datalek zit, zal hij of zij vaak over nuttige informatie beschikken. Voorbeelden van ontdekkers zijn onder meer:

- Een systeembeheerder die een gat in de beveiliging van een systeem met persoonsgegevens op het spoor komt.
- Een callcentermedewerker die van een klant te horen krijgt dat deze via een klantportaal ook inzage heeft in de persoonsgegevens van een andere klant.
- De medewerker die tot de ontdekking komt dat hij of zij een zakelijke laptop met daarop een omvangrijk klantenbestand in de trein heeft laten liggen.

Het is zaak dat de ontdekker wordt aangespoord om juiste en volledige informatie aan de melder te verstrekken zodat geen kostbare tijd verloren gaat. Zorg dat hiervoor een duidelijke procedure is ingericht.

Over het moment van ontdekken valt te discussiëren. Is het redelijk om van bijvoorbeeld de klantenservice medewerker te verwachten dat deze kan inschatten wanneer het incident een meldplichtig datalek is? Vaak zal dat niet het geval zijn. Of ontdek je de meldplichtigheid pas wanneer het beveiligingsincident wordt beoordeeld door bijvoorbeeld een privacyfunctionaris, die gericht een inschatting kan maken of er persoonsgegevens verloren zijn gegaan of onrechtmatig zijn verwerkt en de impact daarvan. Gelukkig biedt de wet nog wel enige mogelijkheid tot het verrichten van onderzoek nadat het beveiligingsincident ontdekt is voordat dit gemeld moet worden, als het een datalek blijkt te zijn. Zo stelt de wet dat een datalek onverwijld gemeld moet worden en hier is door de AP invulling aan gegeven. Zij stelt dat onverwijld betekent binnen 72 uur na het ontdekken. Het is dus zaak dat iedere medewerker binnen de organisatie bekend is met het fenomeen datalek en dat medewerkers ook weten wat er van hen wordt verwacht wanneer ze ermee geconfronteerd worden.

Naast de ontdekker binnen de organisatie kan er ook sprake zijn van een situatie waarbij de ontdekker een persoon is buiten de organisatie zoals bijvoorbeeld een leverancier. In die gevallen is het nog belangrijker voor de organisatie die de rol van verwerkingsverantwoordelijke heeft om ervoor te zorgen dat de (sub)verwerker in de rol van ontdekker weet wat er van hem of haar verwacht wordt. Om dit risico af te kunnen dekken is het aan te raden strikte bepalingen omtrent datalekken en de afhandeling ervan op te nemen in de verwerkersovereenkomst.

Technicus

De technicus is degene die de melder kan helpen met:

- De beantwoording van de vraag welke typen persoonsgegevens gelekt zijn.
- De beantwoording van de vraag wanneer het datalek heeft plaatsgevonden (incl. inzage in of analyse van logfiles).
- De beantwoording van de vraag of de data beveiligd is door bijvoorbeeld versleuteling of anderszins onbegrijpelijk is gemaakt voor derden en op welke wijze dit is gerealiseerd.
- Het repareren van het datalek.
- Voor overige technische vragen.

De melder moet aan de hand van de informatie die hij of zij van de ontdekker ontvangt, snel kunnen vaststellen welke technicus betrokken moet worden bij de afhandeling van het datalek. Dit zou bijvoorbeeld kunnen door een overzicht op te stellen van de aanwezige systemen en de daarbij behorende technicus. Verder is het aan te raden ook de in dit systeem aanwezige persoonsgegevens te vermelden, zodat de melder hierop kan anticiperen.

Melder

De melder is de spin in het web van de (formele) afhandeling van het beveiligingsincident en het mogelijke datalek; het is de medewerker die alle benodigde informatie verzamelt of vaststelt. Aan de hand hiervan bepaalt hij of zij of gemeld moet worden aan de AP of niet. En zo ja, of eveneens aan de betrokkenen gemeld moet worden dat zijn of haar persoonsgegevens zijn gelekt. De melder is ook degene die deze melding bij de AP daadwerkelijk doet en zorgt voor archivering van de melding.

Deze rollen sluiten elkaar niet uit: de ontdekker, maar vooral de technicus en melder kunnen, zeker in een kleine organisatie, één en dezelfde persoon zijn. De rol van ontdekker zal niet van tevoren toegewezen kunnen worden aan een medewerker. Deze rol kiest de medewerker in plaats van andersom, aangezien vrijwel iedere medewerker een datalek zou kunnen ontdekken. De rollen van de technicus en melder kunnen vaak wel op voorhand worden toegewezen en dit is ook aan te raden. Bij kleine bedrijven zal de rol van de technicus bij één medewerker of een kleine groep medewerkers berusten. In grote organisaties zal per systeem of groep systemen één technicus aangewezen moeten worden. De melder zal een coördinerende rol gaan spelen in de afhandeling van een beveiligingsincident of mogelijk datalek.

Standaardprocedure meldplicht datalekken: zes fases

In de afhandeling van een beveiligingsincident en mogelijk datalek kunnen zes fases worden onderscheiden. Deze fases zijn niet per se strikt van elkaar gescheiden en de volgorde staat – uitzonderingen daargelaten - evenmin vast. De fases zijn:

1. Ontdekken;
2. Inventariseren;
3. Kwalificeren;
4. Repareren;
5. Melden;
6. Archiveren.

1. Ontdekken

Iemand moet een beveiligingsincident en daarmee een mogelijk datalek op het spoor komen: de ontdekker. De ontdekker is waarschijnlijk goed in staat om een aantal relevante feiten aan de melder mee te delen. Dit is een belangrijk moment in afhandeling van het beveiligingsincident of mogelijk datalek. De ontdekker moet dan wel weten welke informatie er van hem of haar verlangd wordt. Welke feiten over het datalek aan melder gerapporteerd moeten worden, moet dus op voorhand vaststaan.

Daarmee wordt voorkomen dat de melder op een later moment voor ontbrekende informatie weer te rade moet gaan bij de ontdekker. De organisatie zal eveneens een modaliteit zoals een incidentenmeldingentool of een vast e-mailadres moeten voorschrijven. Zodat de meldingen op één centraal punt binnenkomen.

Het is voor de ontdekker doorgaans lastig om in te schatten of het door hem ontdekte beveiligingsincident een datalek is. Daarom is het aan te raden om een ruime marge te nemen en ieder beveiligingsincident door ontdekker als (mogelijk) datalek te laten rapporteren. Of er daadwerkelijk sprake is van een meldplichtig datalek, zal worden bepaald door de melder aan de hand van een beslissingsschema datalekken. In de bijlage van dit document is een voorbeeld gegeven voor een dergelijk beslissingsschema.

Het is wenselijk dat, voor zover mogelijk, de hierna genoemde informatie door de ontdekker wordt verstrekt aan de melder. Dit kan worden aangevuld door de technicus en de melder zelf. De vraag

over de verantwoordelijkheid moet bijvoorbeeld doorgaans door de melder worden beantwoord. Wanneer de organisatie bij alle incidenten een dergelijk formulier hanteert, ontstaat er uniformiteit in de afhandeling van een beveiligingsincident of mogelijk datalek. Het gaat om de volgende informatie:

- De samenvatting van het incident.
- Het aantal betrokkenen en van wie zijn de persoonsgegevens gelekt.
- Een omschrijving van de groep betrokkenen (klanten, medewerkers, etc.).
- Welke persoonsgegevens gelekt zijn (NAW-gegevens, IBAN, bijzondere of gevoelige gegevens, etc.).
- Of de eigen organisatie als verwerkingsverantwoordelijke of verwerker aan te merken is.
- Wanneer het datalek is ontstaan.
- Wat de oorzaak is van het datalek.
- Welke technische en/of organisatorische maatregelen er getroffen zijn om het datalek te dichten, en/of in de toekomst te kunnen voorkomen.

2. Inventariseren

Naast de gegevens die melder ontvangt van ontdekker, zal het in sommige gevallen nodig zijn om aanvullende informatie omtrent het datalek te verzamelen. Deze informatie is nodig om af te wegen of er wel of geen verplichting is tot het melden van het datalek bij de AP en eventueel bij de betrokkenen. Het grootste gedeelte van de nog ontbrekende informatie zal van technische aard zijn. De melder zal bij de technicus te rade moeten gaan voor deze informatie. Zoals hiervoor vermeld, is het dan ook aan te raden om het bovenstaande schema uit te zetten bij de technicus. Op die manier kan de technicus aanvullen waar relevant en/of noodzakelijk.

Wanneer contact gelegd wordt met de technicus in kwestie, zal deze direct de opdracht moeten krijgen om het beveiligingsincident/mogelijk datalek te (laten) repareren. De technicus zal de melder op de hoogte moeten houden van de ontwikkelingen hieromtrent.
De melder zal in het beheersysteem een nieuwe case aan moeten maken en alle informatie over het beveiligingsincident/datalek hierin moeten opnemen. Het schema is daarmee ook een goed uitgangspunt om zoveel mogelijk informatie direct tot je beschikking te hebben.

3. Kwalificeren

Wanneer de feiten zijn verzameld, kan de melder bepalen of het beveiligingsincident een datalek is en of het gemeld moet worden aan de AP en eventueel aan de betrokkenen. Dit gebeurt aan de hand van het beslissingsschema datalekken. De uitkomst van deze kwalificatie moet eveneens in het beheersysteem worden opgenomen. In de bijlage staat een voorbeeld van een dergelijk beslisschema.

4. Repareren

Onafhankelijk van de uitkomst van fase 3, zullen er maatregelen getroffen moeten worden om het beveiligingsincident/mogelijk datalek te dichten en ook eventueel te voorkomen in de toekomst. Dit gebeurt door de technicus. De technicus moet de melder op de hoogte houden van de vooruitgang. Dit kunnen initiële maatregelen zijn om de directe impact te kunnen beperken, zoals het tijdelijk blokkeren van een klantportaal wanneer er in het klantportaal gegevens zichtbaar zijn van een andere klant. Daarnaast moet er ook gewerkt worden aan structurele maatregelen zodat een dergelijk beveiligingsincident/mogelijk datalek onder gelijkblijvende omstandigheden zich in de toekomst niet nogmaals voordoet.

5. Melden

Indien het datalek onder de meldplicht valt, zal het moeten worden gemeld. De meldplicht is tweeledig: naast dat gemeld moet worden aan de AP, moet onder voorwaarden ook aan de

betrokkenen gemeld worden. De melder heeft reeds onder stap 3 bepaald of en aan wie gemeld moet worden. De melder is ook degene die belast is met het daadwerkelijk doen van de melding. Het afschrift van de gedane melding, het meldingsnummer en de ontvangstbevestiging moeten in het beheersysteem worden ondergebracht.

6. Archiveren

Wanneer de zaak is afgerond, moet het één en ander worden gearchiveerd. De meeste informatie is reeds in het beheersysteem ondergebracht.

Beheersysteem

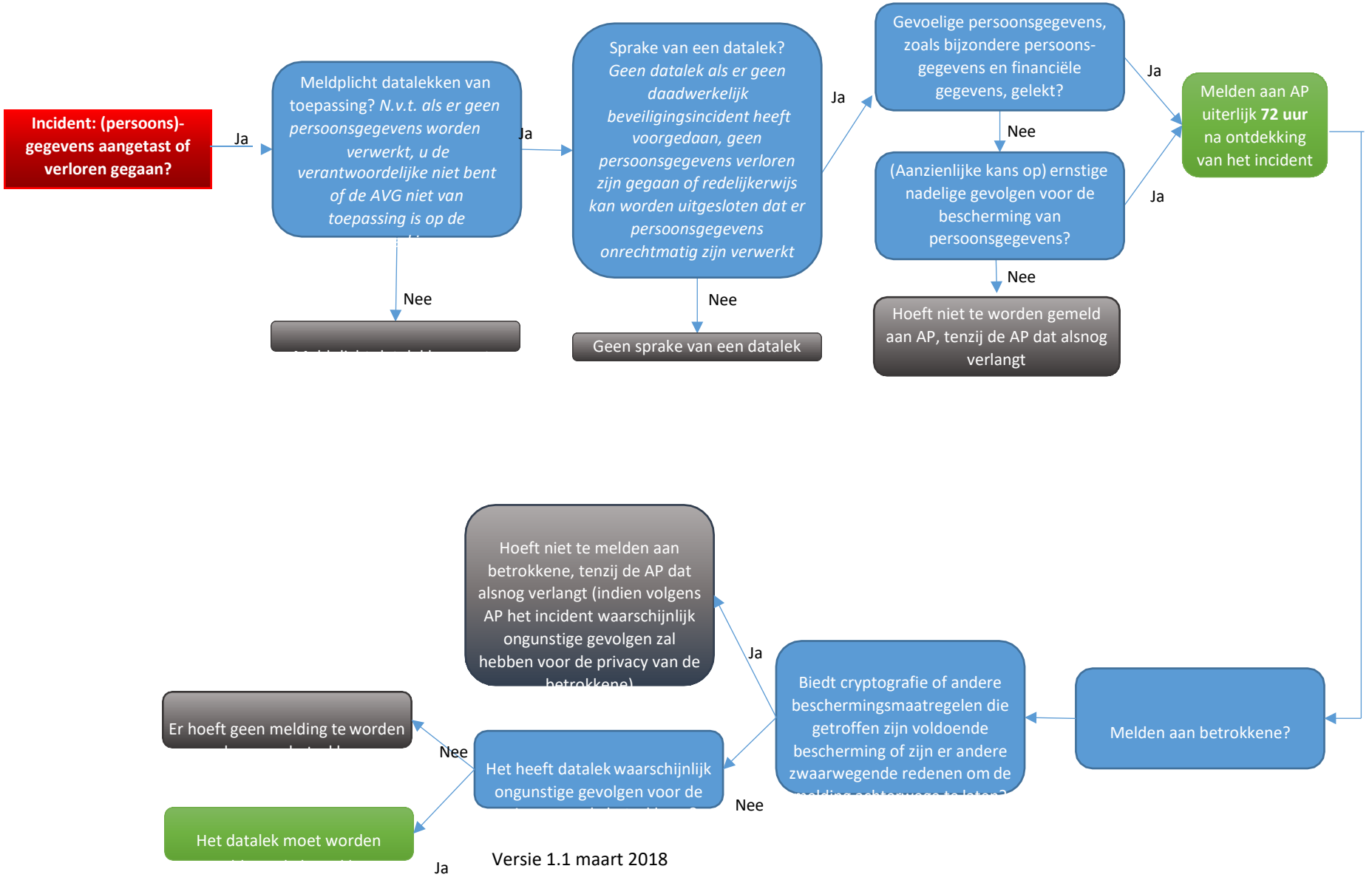
Van belang is dat alle informatie over een beveiligingsincident en/of mogelijk datalek, op een centrale plek wordt vastgelegd. Bijvoorbeeld in wat hierboven steeds met de term beheersysteem is aangeduid (het meldingsregister).

Deze vastlegging dient twee doelen:

- De melder houdt overzicht over de lopende zaken. Er zijn nogal wat variabelen bij de afhandeling van een datalek. Zeker wanneer er mee dan één datalek tegelijk is, is het van belang om overzicht te kunnen houden.
- Incidenten die onder het begrip datalek vallen, dienen te worden gedocumenteerd. De AP mag de documentatie van datalekken opvragen om naleving van de privacyverordening te controleren.

Zoals reeds vermeld is, zijn de bovenstaande zes fases niet statisch. Sterker nog: het is heel belangrijk om de volgorde niet strikt te volgen. Het is een leidraad om weer te geven waar in ieder geval bij stil moet worden gestaan. De fases 1 tot en met 4 lopen eigenlijk meestal tegelijkertijd.

Bijlage: **voorbeeld beslisschema datalekken**



BiSC en Cubiss VIA-Toolkit

12b. Meldplicht datalekken: sjabloon

Privacybeleid BLIJ. Bijlage 7. Meldformulier datalekken

Inleiding

Dit sjabloon voor een register voor datalekken helpt de gebruiker om een register van meldingen van datalekken op de juiste manier op te bouwen en daarmee te voldoen aan één van de verplichtingen van de AVG.

Invulinstructie
Het sjabloon voor het register meldplicht datalekken binnen de Toolkit is opgesteld in MS Excel. De gebruiker dient twee tabbladen in te vullen.

Tabblad 1: Algemene Informatie
Dit blad bevat alleen informatie over degene die de vragenlijst invult en degene die de antwoorden bevestigt/vaststelt. Met die informatie is op elk moment na te gaan bij wie iemand terecht kan met vragen of voor nadere informatie.

Tabblad 2: Register datalekken
Elke melding wordt geregistreerd onder een eigen dossiernummer. Voorts wordt voor de melding de beschikbare informatie conform de kolom-koppen ingevoerd en geüpdatet naar gelang informatie beschibaar is.