Privacyreglement

Stichting Burgerkracht Limburg

Artikel 1 Begripsdefinities

In dit reglement worden de hierna volgende begrippen als volgt gedefinieerd:

Burgerkracht
De stichting Burgerkracht Limburg.

Persoonsgegevens
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand c.q. een (in leven zijnde) persoon gaat, ofwel naar deze persoon te herleiden is.

Algemene Verordening Gegevensbescherming (AVG)
In deze verordening worden regels vastgesteld betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens. Het is een verordening die van toepassing is op de verwerking van persoonsgegevens van betrokkenen die zich in de Europese Unie bevinden in het kader van activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Europese Unie, ongeacht of de verwerking in de Europese Unie plaatsvindt.

Verwerken van persoonsgegevens
Verwerken heeft betrekking op iedere handeling of geheel van handelingen die met de persoonsgegevens verricht kunnen worden, vanaf de verzameling tot aan het moment van vernietiging. De verwerking kan zowel op een geautomatiseerde wijze als op een handmatige wijze verricht worden. In de AVG wordt een niet-limitatieve opsomming gegeven van handelingen die als een verwerking kunnen worden aangemerkt. Enkele handelingen die onder meer worden opgenoemd zijn: het verzamelen, vastleggen, bijwerken, wijzigen, opvragen, gebruiken, verstrekken, het afschermen, uitwissen of vernietigen van gegevens.

Verwerkingsverantwoordelijke
De verwerkingsverantwoordelijke is de entiteit die verantwoordelijk is voor de naleving van de verplichtingen, waaraan voldaan moet worden voor een rechtmatige verwerking van persoonsgegevens. De verwerkingsverantwoordelijke beslist over het gebruik van de persoonsgegevens in haar bestanden (digitaal en hard-copy) en bepaalt de verwerkingsdoelen en de middelen om die doelen te bereiken.

Beheerders
Degenen die verantwoordelijk zijn voor het goed functioneren van (een deel van) het privacyreglement. Zij dragen zorg voor het beheer van persoonsgegevens, de naleving van dit reglement en dragen er zorg voor dat de gegevens slechts ter beschikking komen van degenen die deze gegevens nodig hebben voor het uitoefenen van hun werkzaamheden. De beheerders van deze gegevens zijn de managers en de algemeen directeur.

Gebruikers
Diegenen binnen Burgerkracht Limburg die het geheel of een gedeelte van de persoonsgegevens in het kader van hun werkzaamheden verwerken en daartoe door de beheerders zijn aangewezen en bevoegd.

Betrokkene(n)
De individu(-en) op wie persoonsgegevens betrekking hebben en die door de betreffende persoonsgegeven(s) geïdentificeerd kan/kunnen worden.

Toestemming (van de betrokkene)
Elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling van de hem/haar betreffende verwerking van persoonsgegevens heeft aanvaard.

Verwerker
De verwerker is een natuurlijke persoon of een rechtspersoon die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreekse gezag te zijn onderworpen. De bewerker of verwerker is een buiten de organisatie van de verantwoordelijke staande persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan en veelal zal het gaan om een persoon of instelling die niet in een hiërarchische relatie tot de verantwoordelijke staat. De verwerker mag de betreffende persoonsgegevens niet voor andere doeleinden gebruiken dan waarvoor de verwerkingsverantwoordelijke middels een verwerkersovereenkomst toestemming heeft gegeven.

Ontvanger
Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt.

Medewerker
Een medewerker is een persoon met een arbeidsovereenkomst of aanstelling of opdracht bij Burgerkracht of de aan Burgerkracht gelieerde organisatie. Ingeval een gelieerde organisatie is Burgerkracht de werkgever en de organisatie die volledige zeggenschap heeft in termen van werkgeverschap.

Derde
Een externe natuurlijke persoon of rechtspersoon, een externe overheidsinstantie, een externe dienst of een ander extern orgaan waarvan persoonsgegevens worden verwerkt in verband met bijvoorbeeld het (aan)leveren van diensten, personeel, service, producten etc.

Bestand
Een bestand is een gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn. De onderlinge samenhang kan blijken uit het gemeenschappelijk doel waarvoor de gegevens worden verwerkt, of uit de omstandigheid dat de gegevens in de praktijk als een geheel worden beschouwd. Daarnaast dient de structuur van een verzameling van gegevens op een zodanige manier te zijn opgezet dat de gegevens gemakkelijk toegankelijk zijn.

Geheel of gedeeltelijk geautomatiseerde gegevensverwerking
Van geautomatiseerde verwerking van persoonsgegevens is sprake als gebruik wordt gemaakt van middelen en methoden van geautomatiseerde gegevensverwerking. Er is sprake van een gedeeltelijke geautomatiseerde verwerking als bij de verwerking ook gebruik wordt gemaakt van handmatige verwerking.

Niet geautomatiseerde verwerking in een bestand of bestemd voor een bestand
De verwerking in een gestructureerd dossier, mits deze gegevens in een bestand zijn opgenomen of bestemd zijn om daarin te worden opgenomen.

Privacy-officer
Deze functionaris ziet toe op de naleving van de AVG binnen de organisatie. De functionaris wordt betrokken bij alle zaken binnen de organisatie met betrekking tot de bescherming van persoonsgegevens. De functionaris adviseert gevraagd en ongevraagd en controleert of de maatregelen en activiteiten in het kader van de verwerking van persoonsgegevens voldoen aan de eisen van de AVG.

Autoriteit Persoonsgegevens (AP)
De toezichthouder in Nederland op het gebruik van persoonsgegevens en de naleving van wet- en regelgevingen omtrent de verwerking van persoonsgegevens door organisaties. De Autoriteit Persoonsgegevens kan bij overtreding van de wet- en regelgeving een bestuurlijke boete opleggen.

Inbreuk in verband met persoonsgegevens (ook wel datalek genoemd)
Een inbreuk op de persoonsgegevens is een inbreuk op de beveiliging zonder dat dit de bedoeling is van de organisatie en die leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens. Een inbreuk in verband met persoonsgegevens dient aan de Autoriteit Persoonsgegevens gemeld te worden tenzij het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Privacy by design en privacy by default
De waarborging van gegevensbescherming door ontwerp en door standaardinstellingen. Privacy bij design gaat er vanuit dat bij nieuwe verwerkingen in een vroeg stadium wordt nagedacht over verschillende aspecten m.b.t. privacy. Van privacy by default is sprake als de standaardinstellingen van een softwareprogramma, app of website zodanig zijn dat een maximale privacy gewaarborgd is.

Privacy impact assessment (PIA)
Een beoordelingsprogramma dat de privacy-risico's van een project of een verwerking in een vroeg stadium op een gestructureerde en heldere manier in beeld brengt. In de AVG wordt dit een "gegevensbeschermingseffectbeoordeling" genoemd en de verwerkingsverantwoordelijke is verplicht deze uit te voeren als een verwerking gelet op de aard, omvang, context en doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Artikel 2 Werkingssfeer van het reglement

Dit reglement is van toepassing op de handelingen van Burgerkracht Limburg en op alle geautomatiseerde persoonsgegevensverwerking evenals de niet-geautomatiseerde persoonsgegevensverwerking, mits deze persoonsgegevens in een bestand zijn opgenomen of bestemd zijn om daarin te worden opgenomen.

Artikel 3 Doel van het verwerken van persoonsgegevens

1.Het doel van het verwerken van de persoonsgegevens is het op rechtmatige wijze vastleggen van de persoonsgegevens van medewerkers, contactpersonen en derden voor zover Burgerkracht die nodig heeft voor haar taken en activiteiten.

2. Burgerkracht Limburg maakt een verklaring op hoe met privacy wordt omgegaan en plaatst deze in ieder geval op haar internetsite en verwijst in analoge en digitale communicatie naar deze privacyverklaring. Zie ook Bijlage 1.

3. Burgerkracht Limburg maakt een privacyverklaring kenbaar voor medewerkers en het personeelshandboek maakt deze verklaring aan de medewerkers kenbaar. Zie Bijlage2.

4.Tot deze taken en activiteiten worden in ieder geval gerekend:
- het voeren van een effectief, efficiënt en rechtmatig personeelsbeleid met bijbehorende personeels- en cliëntenadministratie en - beheer;
- de uitvoering van overige wet- en regelgeving en/of het voldoen aan overige wettelijke verplichtingen;
- de uitvoering van de overige publiekrechtelijke taken.

Artikel 4 Bevoegdheid

1.De (verwerkings-)verantwoordelijke is bevoegd het beheer van de bestanden op te dragen aan een beheerder en/of gebruiker en/of verwerker middels machtiging.

2.Een beheerder en/of gebruiker wordt geautoriseerd voor het gebruik van (een gedeelte van) het bestand en/of het systeem. Middels deze autorisatie worden de gegevens uit het bestand uitsluitend verstrekt aan een beheerder en/of gebruikers voor zover zij daartoe bevoegd zijn uit hoofde van hun functie of uit te voeren taken.

3.De verantwoordelijke is bevoegd het beheer van de bestanden op te dragen aan een verwerker. Een verwerker moet voldoen aan de eisen die zijn vastgelegd in artikel 10 van dit reglement en aan de eisen en verplichtingen die zijn gesteld in de verwerkersovereenkomst conform artikel 11 van dit reglement.

Artikel 5 Categorieën van betrokkenen

De persoonsgegevens die worden verwerkt binnen Burgerkracht kunnen betrekking hebben op medewerkers of voormalige medewerkers, derden, stagiaires en vrijwilligers.

Artikel 6 Verkrijging van persoonsgegevens en informatieplicht

1.De persoonsgegevens van betrokkenen worden verwerkt op een rechtmatige, behoorlijke en transparante wijze die verenigbaar is met de doeleinden waarvoor ze zijn verkregen.

2.De persoonsgegevens kunnen worden verkregen van de betrokkene zelf of op een andere wijze dan van betrokkene zelf.

3.Bij het verkrijgen van de persoonsgegevens rechtstreeks van betrokkene wordt vooraf aan de betrokkene medegedeeld:
- de identiteit en contactgegevens van de organisatie (naam);
- de doeleinden van de verwerking waarvoor de gegevens zijn bestemd, alsook de rechtsgrond voor de verwerking (en een toelichting daarop als de rechtsgrond gerechtvaardigd belang is);
- de contactgegevens van de functionaris gegevensbescherming;
- de termijnen van opslag van de persoonsgegevens of de criteria voor de bepaling van die termijnen;
- welke categorieën van persoonsgegevens worden verwerkt;
- de categorieën van ontvangers van de persoonsgegevens;
- de rechten van betrokkene;
- het recht van betrokkene om een klacht in te dienen bij de Autoriteit Persoonsgegevens;
- eventuele verstrekking aan een derde van de persoonsgegevens;
- de eventuele noodzaak van de verwerking van de persoonsgegevens voor het uitvoeren van een wettelijke verplichting.

4.Indien de persoonsgegevens op een andere wijze worden verkregen (bijvoorbeeld van een derde) geldt de informatieplicht op het moment dat de gegevens worden vastgelegd, maar uiterlijk binnen een maand.

5.Het voldoen aan de informatieplicht is niet nodig na toezending of uitreiking van de informatie zoals genoemd in artikel 6 lid 3 van dit artikel, of als er een gerechtvaardigd vermoeden is dat betrokkene reeds op de hoogte is. Dit vermoeden moet blijken uit verklaringen of gedragingen die in het maatschappelijk verkeer aan betrokkene kunnen worden toegerekend als blijk van het feit dat hij op de hoogte is.

6.Informatieverstrekking is niet van toepassing indien de mededeling van de informatie aan de betrokkene onmogelijk blijkt of een onevenredige inspanning kost. Tevens is

informatieverstrekking niet van toepassing indien de vastlegging of de verstrekking bij of krachtens de wet is voorgeschreven. In deze gevallen wordt de herkomst van de gegevens vastgelegd.

7.Nadere informatieverstrekking is aan de orde voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan gemaakt wordt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.

Artikel 7 Verdere verwerking van persoonsgegevens

1.De persoonsgegevens worden na het verzamelen ervan slechts verder verwerkt op een wijze die rechtmatig en verenigbaar is met de doeleinden waarvoor ze zijn verkregen zoals genoemd in artikel 3.

De verdere verwerking van persoonsgegevens dient, gelet op de doeleinden, toereikend, ter zake dienend, niet bovenmatig, juist en nauwkeurig te zijn.

2.De verwerking van persoonsgegevens blijft achterwege voor zover een geheimhoudingsplicht uit hoofde van ambt, beroep of wettelijk voorschrift daaraan in de weg staat.

Artikel 8 Verstrekking van persoonsgegevens aan derden

1.Persoonsgegevens kunnen slechts aan derden verstrekt worden:
- indien betrokkene voor de verstrekking zijn ondubbelzinnige schriftelijke toestemming heeft verleend, of;
- de verstrekking noodzakelijk is voor de uitvoering van een overeenkomst waarbij betrokkene partij is, of;
- voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst, of;
- de gegevensverstrekking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is, of;
- de gegevensverstrekking noodzakelijk is ter vrijwaring van vitaal belang van de betrokkene, of;
- de gegevensverstrekking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt, of;
- de gegevensverstrekking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt,

tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op de bescherming van de persoonlijke levenssfeer, prevaleert.

2.Van alle verzoeken om verstrekking van gegevens aan derden en de besluitvorming daaromtrent, wordt aantekening gehouden in het dossier.

Artikel 9 Documentatieplicht

1.In het kader van de documentatieplicht dient de verantwoordelijke alle processen inzake de gegevensverwerking te documenteren c.q. te bewaren (deze verplichting vervangt de meldplicht bij de AP).

2.Aan deze documentatieplicht wordt voldaan door het opstellen en onderhouden van een “verwerkingenregister” conform art. 30 AVG en beschrijft in ieder geval de volgende informatie:
- de naam en de contactgegevens van de verantwoordelijke;
- de naam en de contactgegevens van de functionaris gegevensbescherming;
- het doel van en de rechtsgrond voor de verwerking van persoonsgegevens;
- een beschrijving van de categorieën van betrokkenen en de categorieën van persoonsgegevens die worden verwerkt;
- de ontvangers van de persoonsgegevens;
- eventuele informatie over doorgifte van persoonsgegevens aan derde landen;
- de termijn of de criteria waarbinnen de gegevens worden gewist;
- een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Artikel 10 De verwerker en de verwerkersovereenkomst

1.De verantwoordelijke draagt zorg dat de verwerker voldoende waarborgen biedt ten aanzien van passende technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen, en ten aanzien van de melding van een inbreuk op de beveiliging, bedoeld in artikel 18 van dit reglement.

2.De verantwoordelijke ziet toe op de naleving van de maatregelen genoemd in artikel 10 lid 1
De uitvoering van verwerkingen door een verwerker en alle verplichtingen van de verwerker worden geregeld in een overeen te komen verwerkersovereenkomst als onderdeel van de hoofdovereenkomst en als bedoeld in artikel 11.

3.De verantwoordelijke mag alleen van een dienst van een verwerker gebruikmaken als de verwerker voldoende garanties biedt dat de verwerking wordt uitgevoerd volgens de regels en verplichtingen opgenomen in dit reglement en in de verwerkersovereenkomst.

Artikel 11 De verwerkersovereenkomst

1.De verwerkersovereenkomst houdt de wijze in waarop de gegevensverwerking door de verwerker plaatsvindt. Een standaard verwerkersovereenkomst is opgenomen in Bijlage 3 van dit reglement.

2.De volgende verplichtingen moeten over en weer duidelijk zijn vastgelegd in de verwerkersovereenkomst:
- welke persoonsgegevens worden verwerkt;
- de doeleinden van de verwerking;
- de duur van de opslag;
- het meewerken aan de verplichtingen m.b.t. de beveiligingsmaatregelen en een beschrijving van de te nemen beveiligingsmaatregelen;
- de wijze waarop datalekken worden gemeld;
- een meewerkplicht aan audits en het ter beschikking stellen van informatie aan de verantwoordelijke;
- het vooraf toestemming vragen aan de verantwoordelijke bij het inschakelen van sub-bewerkers, en;
- een plicht tot het verwijderen of teruggeven van persoonsgegevens na afloop van de dienstverlening.

3.In de overeenkomst moet worden opgenomen hoe de verantwoordelijke kan toezien op de naleving van de waarborgen.
4.De overeenkomst bevat een geheimhoudingsplicht voor de verwerker en zijn personeel.

Artikel 12 Bewaren van persoonsgegevens

1.Persoonsgegevens worden niet langer bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld en verwerkt.

2.De (minimale en maximale) bewaartermijnen van bepaalde voor de organisatie relevante documenten c.q. bestanden zijn vastgesteld in Bijlage 4 van dit reglement.

3.Indien aan een bepaalde wettelijk bewaarplicht moet worden voldaan is het toegestaan gegevens langer te bewaren dan de (minimale en maximale) termijnen genoemd in bijlage 4 van dit reglement.

4.Indien de gegevens langer bewaard worden om daar een gerechtvaardigd belang van Burgerkracht mee te dienen, dan heeft een zorgvuldige afweging plaats gehad van de

criteria en de overwegingen voor deze keuze. Deze afweging is separaat vastgelegd.

5.Zijn de in Bijlage 4 opgenoemde termijnen verlopen, dan mogen de gegevens niet meer verwerkt worden, tenzij voor een ander, daarmee verenigbaar doel.

6.Indien persoonsgegevens niet meer noodzakelijk zijn voor de verwerkelijking van de doeleinden waarvoor ze zijn verzameld, worden deze gegevens vernietigd.

Artikel 13 Gebruik persoonsgegevens voor onderzoek en/of statistiek

1.Persoonsgegevens worden langer bewaard dan bepaald in artikel 12 voor zover deze voor historische, statistische of wetenschappelijke doeleinden dienen te worden bewaard en de verantwoordelijke de nodige voorzieningen heeft getroffen ten einde te verzekeren dat de desbetreffende gegevens uitsluitend voor deze specifieke doeleinden worden gebruikt.

2.Betrokkene wordt van tevoren in algemene zin geïnformeerd over het feit dat de gegevens gebruikt kunnen worden voor onderzoek en/of voor statistiek. Betrokkene heeft hiertegen geen uitdrukkelijk bezwaar gemaakt.

Artikel 14 Geheimhoudingsplicht persoonsgegevens en beveiliging

1.Eenieder die de beschikking krijgt over persoonsgegevens waarvan hij het vertrouwelijk karakter kent of redelijkerwijs moet vermoeden en voor wie niet reeds uit hoofde van functie, beroep of wettelijk voorschrift ter zake van die gegevens een geheimhoudingsplicht geldt, is verplicht tot geheimhouding daarvan, behoudens voor zover enig (wettelijk) voorschrift en/of een gerechtvaardigd toegelicht doel en/of missie hem tot bekendmaking verplicht.

2.De beheerder, systeembeheerder en de applicatiebeheerder dragen de zorg voor het aanleggen van passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen.

3.Een gelijke plicht zoals genoemd in lid 2 van dit artikel ligt op de gebruikers ten aanzien van de door hen te gebruiken persoonsgegevens.

4.De privacy-maatregelen genoemd in de artikelen 15 tot en met 17 maken onderdeel uit van de beveiliging.

5.Periodiek wordt getoetst of de genomen maatregelen voor beveiliging nog adequaat zijn gezien de omstandigheden van het geval.

Artikel 15 Privacy by design en privacy by default

1.De privacy by design en default waarborgt de gegevensbescherming in ontwerp en in standaardinstellingen. Zo wordt erop toegezien dat met de producten en diensten die binnen Burgerkracht worden gebruikt de bescherming van de privacy vanaf het begin van een proces wordt ingebouwd.

2.Deze maatregel wordt toegepast vanaf de bepaling van de verwerkingsmiddelen alsook bij het gehele proces van verwerking van gegevens.

Artikel 16 Privacy impact assessment (PIA)

1.Bij bijzonder risicovolle verwerkingen stelt de verantwoordelijke een 'privacy impact assessment' ("gegevensbeschermingseffectbeoordeling") vast, zodat bepaalde risico's van een project/activiteit/werkzaamheden in een vroeg stadium op een gestructureerde en heldere manier in beeld worden gebracht.

2.De Privacy impact assessment kan worden uitgevoerd door een opdrachtgever, een opdrachtnemer of een functionaris van Burgerkracht. Wanneer een privacy-officer voor gegevens- bescherming is aangewezen, wint Burgerkracht diens advies in.

Artikel 17 Privacy-officer

1.De privacy-officer is onafhankelijk, niet gebonden aan eventuele instructies van de verantwoordelijke en is gehouden aan de geheimhoudingsplicht conform artikel 14 lid 1.

2.Binnen Burgerkracht heeft de privacy-officer de volgende taken:
- de functionaris informeert en adviseert het management en de medewerkers over de verplichtingen op grond van de Algemene verordening gegevensbescherming;
- de functionaris ziet toe op de naleving van de Verordening en het privacybeleid van Burgerkracht;
- de functionaris adviseert op verzoek van de directie over de Privacy Impact Assessment (PIA) en ziet toe op de uitvoering daarvan;

- de functionaris werkt samen met en treedt op als contactpersoon voor de Autoriteit Persoonsgegevens
- de functionaris rapporteert over de uitvoering van zijn taken aan de directie en het management;
- de functionaris draagt zorg voor een toename van het bewustzijn van privacy binnen de organisatie.

3.De functionaris wordt tijdig en behoorlijk betrokken bij alle aangelegenheden die verband houden met de bescherming van de persoonsgegevens en wordt door de organisatie ondersteund in de uitvoering van zijn taken.

4.Betrokkenen kunnen zich via privacy@burgerkrachtlimburg.nl wenden tot de privacy-officer voor alle aangelegenheden die verband houden met de privacy.

Artikel 18 Meldplicht van een inbreuk in verband met persoonsgegevens (datalek)

1.Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de verwerkingsverantwoordelijke deze zonder onredelijke vertraging, indien mogelijk binnen 72 uur, aan de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

2.De verantwoordelijke dient ook onverwijld een melding te doen aan de betrokkene, indien het datalek waarschijnlijk een hoog risico inhoudt voor diens persoonlijke levenssfeer, rechten en vrijheden.

3.Binnen Burgerkracht wordt bij een datalek gehandeld te worden conform het Datalekprotocol , zoals opgenomen in Bijlage 5 van dit reglement.

Artikel 19 Recht op inzage en recht op een afschrift

1.Betrokkene kan met redelijke tussenpozen een verzoek tot inzage of een verzoek tot afgifte van een afschrift van zijn persoonsgegevens indienen bij de verantwoordelijke.

2.Het indienen van een verzoek tot inzage of een verzoek om een afschrift te verkrijgen geschiedt schriftelijk, waarna de verantwoordelijke een besluit neemt of dit wel of niet wordt toegestaan. Bij weigering zal dit in een gemotiveerd besluit aan betrokkene kenbaar worden gemaakt, waarna betrokkene binnen zes weken na ontvangst van het besluit hiertegen een bezwaar c.q. klacht kan indienen.

3.Inzage vindt altijd plaats onder begeleiding van de behandelend functionaris. Zo nodig kan door deze functionaris een toelichting worden gegeven.

4.Betrokkene kan, indien hij dit wenst, kopieën laten maken van de aanwezige stukken. Bij het verstrekken van afschriften wordt op het document aangegeven dat het een kopie betreft.

5.Burgerkracht is gerechtigd voor de verstrekking van afschriften een kostprijs in rekening te brengen als de betrokkene meerdere kopieën van dezelfde persoonsgegevens in hetzelfde verzoek vraagt.

6.Alle verzoeken tot inzage en het ontvangen van een afschrift van persoonsgegevens en de besluitvorming hieromtrent worden gedocumenteerd.

Artikel 20 Recht op beperking van de verwerking

1.Betrokkene kan de verantwoordelijke verzoeken om de verwerking van hem betreffende persoonsgegevens te beperken indien:
- betrokkene gemotiveerd de juistheid van de persoonsgegevens betwist;
- de verwerking aantoonbaar onrechtmatig is;
- de verantwoordelijke de persoonsgegevens niet meer nodig heeft en wil wissen, maar betrokkene deze persoonsgegevens wel nodig heeft voor een andere organisatie, voor een onderbouwing of voor de uitoefening van een rechtsvordering;
- de betrokkene bezwaar heeft gemaakt tegen de verwerking en in afwachting is van het antwoord op de vraag of de gerechtvaardigde gronden van verantwoordelijke zwaarder wegen dan die van de betrokkene.

2.Het indienen van een verzoek tot beperking van de verwerking van persoonsgegevens geschiedt schriftelijk, waarna de verantwoordelijke een besluit neemt of dit wel of niet wordt toegestaan. Bij weigering zal dit in een gemotiveerd besluit aan betrokkene kenbaar worden gemaakt, waarna betrokkene binnen zes weken na ontvangst van het besluit hiertegen een bezwaar c.q. klacht kan indienen.

3.Alle verzoeken tot beperking van de verwerking van persoonsgegevens en de besluitvorming hieromtrent worden gedocumenteerd.

Artikel 21 Recht op beperking van de verwerking

1.Indien persoonsgegevens op een geautomatiseerde wijze zijn verwerkt kan betrokkene de verantwoordelijke verzoeken om de betreffende persoonsgegevens over te dragen van het

ene elektronische platform naar het andere, waardoor persoonsgegevens worden overgedragen aan een andere verantwoordelijke (dit is dataportabiliteit).

2.Het indienen van een verzoek tot dataportabiliteit geschiedt schriftelijk, waarna de verantwoordelijke een besluit neemt of dit wel of niet wordt toegestaan. Bij weigering zal dit in een gemotiveerd besluit aan betrokkene kenbaar worden gemaakt, waarna betrokkene binnen zes weken na ontvangst van het besluit hiertegen een bezwaar c.q. klacht kan indienen.

3.Alle verzoeken tot dataportabiliteit van persoonsgegevens en de besluitvorming hieromtrent worden gedocumenteerd.

Artikel 22 Recht van correctie/rectificatie

1.Betrokkene kan de verantwoordelijke verzoeken zijn persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn, dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt.

2.Het indienen van een verzoek tot correctie/rectificatie geschiedt schriftelijk, waarna de verantwoordelijke een besluit neemt of dit wel of niet wordt toegestaan. Bij weigering zal dit in een gemotiveerd besluit aan betrokkene kenbaar worden gemaakt, waarna betrokkene binnen zes weken na ontvangst van het besluit hiertegen een bezwaar c.q. klacht kan indienen.

3.Alle verzoeken tot correctie/rectificatie van persoonsgegevens en de besluitvorming hieromtrent worden gedocumenteerd.

Artikel 23 Uitzonderingen

De toepassing van artikel 6 lid 2 tot en met lid 7, artikel 7 lid 1, en de artikelen 8, 19, 20, 21 en 22 kan achterwege blijven voor zover dit noodzakelijk is in het belang van:
- de veiligheid van de staat;
- de voorkoming, opsporing en vervolging van strafbare feiten;
- gewichtige economische en financiële belangen van de staat en andere openbare lichamen;
- het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de belangen onder het tweede en derde gedachtestreepje van dit artikel of;
- de bescherming van betrokkene of van de rechten en vrijheden van anderen.

Artikel 24 Benaming

Dit reglement wordt aangehaald als het PRIVACYREGLEMENT STICHTING BURGERKRACHT LIMBURG.

Artikel 25 Bekendmaking

Bekendmaking van dit reglement geschiedt door publicatie van het privacyreglement en door opname van het reglement op haar internetsite, op intranet en in het organisatiehandboek van Burgerkracht.

Artikel 26 Intrekking

1.Tegelijkertijd met de vaststelling van het privacyreglement met betrekking tot de bescherming van persoonsgegevens worden ingetrokken:
- de privacyverklaring van 25 mei 2018 zoals gepubliceerd op de website van Burgerkracht.

Artikel 27 Inwerkingtreding

Het privacyreglement met betrekking tot de bescherming van persoonsgegevens treedt in werking op de eerste dag na publicatie.

Aldus vastgesteld op 22 juli 1997 na verkregen instemming van de
PVT 1 juli 2019.

J.H.M. von den Hoff
Directeur - bestuurder

Bijlage 1: Privacyverklaring Stichting Burgerkracht Limburg

Stichting Burgerkracht Limburg (hierna Burgerkracht Limburg) verwerkt uw persoonsgegevens op een veilige en zorgvuldige manier waardoor uw gegevens in principe niet in handen kunnen komen van onbevoegden. Wij waarderen uw vertrouwen in onze stichting en voldoen in de behandeling van uw persoonsgegevens tenminste aan de eisen van de Algemene Verordening Gegevensbescherming (AVG/GDPR). Hieronder leest u hoe wij daar concreet invulling aan geven.

Persoonsgegevens die wij verwerken
Burgerkracht Limburg verwerkt persoonsgegevens over u doordat u gebruik maakt van onze diensten en/of omdat u deze zelf aan ons verstrekt. Door gebruik te maken van deze diensten gaat u ermee akkoord dat wij uw persoonsgegevens verzamelen en gebruiken in overeenstemming met deze privacyverklaring. Hieronder een overzicht van de persoonsgegevens die wij, mogelijkerwijs, verwerken. Mogelijkerwijs wil zeggen dat wij niet in alle gevallen over al deze gegevens beschikken:

- *Voor- en achternaam*
- *Geslacht*
- *Geboortedatum*
- *Geboorteplaats*
- *Adresgegevens*
- *Telefoonnummer*
- *E-mailadres*
- *Overige persoonsgegevens die u actief verstrekt bijvoorbeeld door een profiel op de Burgerkracht- website aan te maken, in correspondentie en telefonisch*
- *IP-adres*
- *Internetbrowser en apparaat type.*

Waarom we uw gegevens nodig hebben
Burgerkracht Limburg verwerkt uw persoonsgegevens, voor de volgende doelen:
ter verzending van onze nieuwsbrief;

- om contact met u op te kunnen nemen indien dit nodig is om onze dienstverlening uit te kunnen voeren;
- om u te informeren over wijzigingen van onze diensten en producten;
- om u te benaderen voor de deelname aan onderzoeken. Deze onderzoeken kunnen ook door derden (bijvoorbeeld een ziekenhuis) worden uitgevoerd.

Hoe lang we gegevens bewaren
Burgerkracht Limburg zal uw persoonsgegevens niet langer bewaren dan strikt nodig is om de doelen te realiseren waarvoor uw gegevens worden verzameld. Wij houden ons uiteraard aan de wettelijk termijnen. Voor de overige termijnen hebben wij in Bijlage 4 van het Privacyreglement stichting Burgerkracht Limburg een overzicht opgenomen.
Indien u heeft ingestemd met een deelname aan een onderzoek, dan zullen wij deze aanmeldgegevens maximaal 7 jaar bewaren. Indien het onderzoek door een derde wordt uitgevoerd (bijvoorbeeld een ziekenhuis), dan vragen wij vooraf altijd uw toestemming.

Delen met anderen
Burgerkracht Limburg verkoopt uw gegevens niet aan derden en zal deze uitsluitend verstrekken indien dit nodig is voor de uitvoering van onze overeenkomst met u of om te voldoen aan een wettelijke verplichting. Met bedrijven die uw gegevens verwerken in opdracht van ons, sluiten wij een bewerkersovereenkomst om te zorgen voor eenzelfde niveau van beveiliging en vertrouwelijkheid van uw gegevens.

In kaart brengen websitebezoek
Burgerkracht Limburg gebruikt functionele en analytische cookies. Een cookie is een klein tekstbestand dat bij het eerste bezoek aan onze website wordt opgeslagen in de browser van uw computer, tablet of smartphone. Burgerkracht Limburg gebruikt cookies met een puur technische functionaliteit. Deze zorgen ervoor dat de website naar behoren werkt, kunnen bijvoorbeeld uw voorkeursinstellingen onthouden en helpen ons om de website goed te laten werken. Ook kunnen wij hiermee onze website optimaliseren.
U kunt zich afmelden voor cookies door uw internetbrowser zo in te stellen dat deze geen cookies meer opslaat. Daarnaast kunt u ook alle informatie die eerder is opgeslagen via de instellingen van uw browser verwijderen. Zie voor een toelichting: https://veiliginternetten.nl/themes/situatie/wat-zijn-cookies/.

Gegevens inzien, aanpassen of verwijderen
U heeft het recht om uw persoonsgegevens in te zien, te corrigeren of te verwijderen. U kunt een verzoek tot inzage, correctie of verwijdering sturen naar privacy@burgerkrachtlimburg.nl. Om er zeker van te zijn dat het verzoek tot inzage door u is gedaan, vragen wij u een kopie van uw identiteitsbewijs bij het verzoek mee te sturen. Hierbij vragen we u om in deze kopie uw pasfoto en Burgerservicenummer (BSN) onzichtbaar te maken. Dit ter bescherming van uw privacy. Deze kopie wordt na controle direct vernietigd.
Burgerkracht Limburg zal zo snel mogelijk, maar binnen vier weken, op uw verzoek reageren.

Beveiliging
Burgerkracht Limburg neemt de bescherming van uw gegevens serieus en neemt adequate technische en organisatorische maatregelen om misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging tegen te gaan. Als u de indruk heeft dat uw gegevens niet goed beveiligd zijn of er aanwijzingen zijn van misbruik, neem dan contact op met ICT – beheer Burgerkracht Limburg. Bovendien heeft u te allen tijde het recht om een klacht of bezwaar in te dienen bij de Autoriteit Persoonsgegevens, Bezuidenhoutseweg 30, 2594 AV Den Haag.

Wijzigingen
Wij kunnen deze Privacyverklaring om uiteenlopende redenen wijzigen door de bijgewerkte versie van de Privacyverklaring op onze website te plaatsen. Wij raden u aan de verklaring regelmatig te bekijken om op de hoogte te blijven van de manier waarop we uw persoonsgegevens gebruiken. De hier getoonde versie is van 22 juli 2019 en vervangt de eerder gepubliceerde versie van 25 mei 2018.

Bijlage 2: Privacyverklaring voor medewerkers en personeelshandboek

Privacyverklaring medewerkers, vrijwilligers en personeelshandboek
Burgerkracht Limburg verwerkt uw persoonsgegevens op een veilige en zorgvuldige manier waardoor uw gegevens in principe niet in handen kunnen komen van onbevoegden. Wij voldoen in de behandeling van uw persoonsgegevens tenminste aan de eisen van de Algemene Verordening Gegevensbescherming (AVG/GDPR). Hieronder leest u hoe wij daar concreet invulling aan geven.

Persoonsgegevens die wij verwerken
Burgerkracht Limburg verwerkt persoonsgegevens van u doordat u een arbeidsovereenkomst of vrijwilligersovereenkomst met ons hebt afgesloten. Door deze overeenkomst gaat u ermee akkoord dat wij uw persoonsgegevens verzamelen en gebruiken in overeenstemming met deze privacyverklaring. Hieronder een overzicht van de persoonsgegevens die wij verwerken:

- *Voor- en achternaam*
- *Geslacht*
- *Geboortedatum*
- *Geboorteplaats*
- *Adresgegevens*
- *Telefoonnummer*
- *E-mailadres*
- *Overige persoonsgegevens die u actief verstrekt bijvoorbeeld t.b.v. de personeelsadministratie*
- *IP-adres*
- *Internetbrowser en apparaat type*
- *Bankrekening (IBAN).*

Bijzondere en/of gevoelige persoonsgegevens die wij verwerken
Burgerkracht Limburg verwerkt de volgende bijzondere en/of gevoelige persoonsgegevens van u:

- *Burgerservicenummer (BSN)*
- *Gegevens van derden ivm inning en incasso (beslag op loon)*

Waarom we uw gegevens nodig hebben
Burgerkracht Limburg verwerkt uw persoonsgegevens voor de volgende doelen:

- Het na kunnen komen van de afspraken in de arbeidsovereenkomst
- Het op een correcte en tijdige manier communiceren met externe partijen zoals belastingdienst, UWV, arbodienst, et cetera in het kader van een wettelijke verplichting daartoe.

Hoe lang we gegevens bewaren
Burgerkracht Limburg zal uw persoonsgegevens niet langer bewaren dan strikt nodig is om de doelen te realiseren waarvoor uw gegevens worden verzameld. Onze bewaartermijn(en) zijn vastgelegd in het document minimale en maximale

bewaartermijnen. Deze is als Bijlage 4 toegevoegd aan het privacyreglement stichting Burgerkracht Limburg. Voor de overige termijnen hebben wij in Bijlage 4 van het Privacyreglement stichting Burgerkracht Limburg een overzicht opgenomen.
Indien de medewerker een alternatieve bewaartermijn van een persoonsgegeven vraagt en de organisatie wenst hier aan te voldoen, dan wordt deze beslissing met beschrijving van de redenen in ieder geval in het verwerkingenregister opgenomen.

Delen met anderen
Burgerkracht Limburg verkoopt uw gegevens niet aan derden en zal deze uitsluitend verstrekken indien dit nodig is voor de uitvoering van onze overeenkomst met u of om te voldoen aan een wettelijke verplichting. Met bedrijven die uw gegevens verwerken in onze opdracht, sluiten wij een verwerkersovereenkomst om te zorgen voor eenzelfde niveau van beveiliging en vertrouwelijkheid van uw gegevens. Burgerkracht Limburg blijft verantwoordelijk voor deze verwerkingen.

Gegevens inzien, aanpassen of verwijderen
U heeft het recht om uw persoonsgegevens in te zien, te corrigeren of te verwijderen. U kunt een verzoek tot inzage, correctie of verwijdering sturen naar privacy@burgerkrachtlimburg.nl. Om er zeker van te zijn dat het verzoek tot inzage door u is gedaan, vragen wij u een kopie van uw identiteitsbewijs bij het verzoek mee te sturen. Hierbij kunt u in deze kopie uw pasfoto en Burgerservicenummer (BSN) zwart maken. Dit ter bescherming van uw privacy. Deze kopie wordt na controle direct vernietigd. Burgerkracht Limburg zal zo snel mogelijk, maar binnen vier weken, op uw verzoek reageren.

Beveiliging
Burgerkracht Limburg neemt de bescherming van uw gegevens serieus en neemt adequate technische en organisatorische maatregelen om misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging tegen te gaan. Als u de indruk heeft dat uw gegevens niet goed beveiligd zijn of er aanwijzingen zijn van misbruik, neem dan contact op met ICT – beheer. Bovendien heeft u te allen tijde het recht om een klacht of bezwaar in te dienen bij de Autoriteit Persoonsgegevens, Bezuidenhoutseweg 30, 2594 AV Den Haag.

Wijzigingen
Wij kunnen deze Privacyverklaring om uiteenlopende redenen wijzigen door de bijgewerkte versie van de Privacyverklaring in het personeelshandboek te plaatsen. Van belangrijke wijzigingen krijgt u persoonlijk bericht. Deze versie is opgemaakt op 22 juli 2019.

Bijlage 2: Model verwerkersovereenkomst

Partijen:

[NAAM KLANT + RECHTSVORM], gevestigd te [plaats, eventueel straat en huisnummer], hierna te noemen: "**Verantwoordelijke**", "**U**" of "**Uw**", ten deze rechtsgeldig vertegenwoordigd door [naam], in diens hoedanigheid van [functie];

en

Stichting Burgerkracht Limburg gevestigd te Sittard, Mercator 1, hierna te noemen: "**Verwerker**" , "**Wij**", "**Ons**" of "**Onze**", te dezen rechtsgeldig vertegenwoordigd door Directeur-bestuurder;

hierna gezamenlijk aangeduid als "Partijen", "We" of "Wij Gezamenlijk"

Overwegingen:

U bent per [evt. datum] gebruiker van onze diensten waarvoor wij met u een overeenkomst afgesloten hebben (de "Onderliggende opdracht"). Wij verwerken daarbij de Persoonsgegevens die vermeld staan in de Bijlage die bij deze Overeenkomst hoort.

Wij zijn aan te merken als "verwerker" en u als "verwerkingsverantwoordelijke". In deze Overeenkomst leggen We onze wederzijdse rechten en verplichtingen vast.

Partijen komen het volgende overeen:

1. Definities

In deze Overeenkomst wordt een aantal begrippen gebruikt. De betekenis van die begrippen is hieronder verduidelijkt. De genoemde begrippen worden in deze Overeenkomst met een hoofdletter geschreven.

Betrokkene:	Degene op wie een persoonsgegeven betrekking heeft.
Verwerker:	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt , zonder aan zijn rechtstreeks gezag te zijn onderworpen.
Sub-verwerker:	Een andere verwerker die door de Verwerker wordt ingezet om ten behoeve van de Verwerkingsverantwoordelijke specifieke verwerkingsactiviteiten te verrichten.

Verwerkingsverantwoordelijke / Verantwoordelijke:	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
Bijzondere Persoonsgegevens:	Dit zijn gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid. Alsmede persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen.
Datalek / Inbreuk in verband met persoonsgegevens:	Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot - of waarbij redelijkerwijs niet uit te sluiten valt dat die kan leiden tot - de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.
Derden:	Anderen dan u en wij en onze medewerkers.
Meldplicht Datalekken:	De verplichting tot het melden van datalekken aan de Autoriteit Persoonsgegevens en (in sommige gevallen) aan betrokkene(n).
Medewerkers	Personen die werkzaam zijn bij U of bij ons, ofwel in dienstbetrekking dan wel tijdelijk ingehuurd.
Onderliggende opdracht:	De opdracht zoals hierboven bedoeld in de overwegingen onder A.
Overeenkomst:	Deze verwerkersovereenkomst.

Persoonsgegevens:	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene") die in het kader van de "onderliggende opdracht" worden verwerkt; als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
Persoonsgegevens van gevoelige aard	Persoonsgegevens waarbij verlies of onrechtmatige verwerking kunnen leiden tot (onder meer) stigmatisering of uitsluiting van Betrokkene , schade aan de gezondheid, financiële schade of tot (identiteits) fraude. Tot deze categorieën van persoonsgegevens moeten in ieder geval worden gerekend: - Bijzondere persoonsgegevens - Financiële of economische gegevens over de betrokkene - Gegevens die kunnen leiden tot stigmatisering of uitsluiting - Gebruikersnamen, wachtwoorden en andere inloggegevens - Gegevens die kunnen leiden tot (identiteits-)fraude.
Verwerken / Verwerking:	Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
AVG:	Algemene Verordening Gegevensbescherming, inclusief de uitvoeringswet van deze verordening. De AVG vervangt de Wet bescherming persoonsgegevens per 25 mei 2018.

2. Toepasselijkheid en looptijd

2.1 Deze overeenkomst is van toepassing op iedere Verwerking die door ons als verwerker wordt gedaan op basis van de onderliggende opdracht, gegeven door U als verantwoordelijke.

2.2 Deze overeenkomst treedt in werking op de datum waarop de onderliggende opdracht van kracht wordt en eindigt op het moment dat wij geen persoonsgegevens meer onder ons hebben die wij in het kader van de onderliggende Opdracht voor u verwerken. Het is niet mogelijk om deze overeenkomst tussentijds op te zeggen.

2.3 Artikel 6 en 7 van deze Overeenkomst blijven gelden, ook nadat de overeenkomst (of de onderliggende opdracht) is geëindigd.

3. Verwerking

3.1 Wij verwerken de persoonsgegevens uitsluitend op de manier die wij met u hebben afgesproken in de onderliggende opdracht. Dit verwerken doen wij niet langer of uitgebreider dan noodzakelijk voor de uitvoering van deze onderliggende opdracht. De verwerking vindt plaats volgens uw schriftelijke instructies, tenzij wij op grond van de wet- of regelgeving verplicht zijn om anders te handelen.
Indien een instructie, naar onze mening, een inbreuk maakt op de AVG, stellen wij U daarvan onmiddellijk in kennis.

3.2 De verwerking vindt plaats onder uw verantwoordelijkheid. Wij hebben geen zeggenschap over het doel en de middelen van de verwerking en nemen geen beslissingen over zaken als het gebruik van persoonsgegevens, de bewaartermijn van de voor u verwerkte persoonsgegevens en het verstrekken van persoonsgegevens aan derden. U dient er voor te zorgen dat u het doel en de middelen van de Verwerking van de persoonsgegevens duidelijk heeft vastgesteld. De zeggenschap over de persoonsgegevens berust nooit bij ons. Als wij een zelfstandige verplichting mochten hebben op basis van wettelijke voorschriften, dan leven wij deze verplichtingen na.

3.3 U bent wettelijk verplicht de vigerende wet- en regelgeving op het gebied van privacy na te leven. In het bijzonder dient u vast te stellen of er sprake is van een rechtmatige grondslag voor het verwerken van de persoonsgegevens. Wij zorgen ervoor dat wij voldoen aan de op ons als verwerker van toepassing zijnde regelgeving op het gebied van de verwerking van persoonsgegevens en de afspraken die We hebben gemaakt in deze overeenkomst.

3.4 Wij schakelen andere verwerkers in (Sub-verwerkers) voor het uitvoeren van bepaalde werkzaamheden die voortvloeien uit de onderliggende opdracht. Als het inschakelen van Sub-Verwerkers tot gevolg heeft dat zij Persoonsgegevens gaan Verwerken, dan zullen wij de Sub-Verwerkers (schriftelijk) de verplichtingen uit deze overeenkomst opleggen. Met ondertekening van deze overeenkomst geeft u toestemming voor het inschakelen van de Sub-Verwerkers die genoemd zijn in de Bijlage die bij deze overeenkomst hoort. Over het inschakelen van overige Sub-Verwerkers zullen wij u vooraf informeren en in de gelegenheid stellen hiertegen bezwaar te maken.

3.5 Wij zorgen ervoor dat alleen onze medewerkers toegang hebben tot de persoonsgegevens. De uitzondering hierop is opgenomen in artikel 3.4. Wij beperken de toegang tot Medewerkers van ons en van Sub-verwerkers voor wie de toegang noodzakelijk is voor hun werkzaamheden, waarbij de toegang beperkt is tot persoonsgegevens die deze Medewerkers nodig hebben voor hun werkzaamheden. Onder noodzakelijk wordt hier verstaan: u of een van uw medewerkers heeft ons schriftelijk of mondeling gevraagd om ondersteuning of rapportage met betrekking tot deze persoonsgegevens.
Wij zorgen er bovendien voor dat de medewerkers die toegang hebben tot de persoonsgegevens een juiste en volledige instructie hebben gekregen over de omgang met persoonsgegevens en dat zij bekend zijn met de verantwoordelijkheden en wettelijke verplichtingen.

3.6 Voor zover mogelijk verlenen wij u bijstand bij het vervullen van uw verplichtingen om verzoeken om uitoefening van rechten van betrokkenen af te handelen. Als wij (rechtstreeks) verzoeken ontvangen van betrokkene(n) om uitoefening van hun rechten (bijvoorbeeld inzage, wijziging of verwijdering van persoonsgegevens), dan zenden wij deze verzoeken door naar u. U handelt deze verzoeken zelf af, waarbij wij u natuurlijk behulpzaam kunnen zijn als wij in het kader van de onderliggende opdracht toegang hebben tot deze persoonsgegevens. Hiervoor kunnen wij kosten in rekening brengen.

3.7 Wij zullen de persoonsgegevens alleen verwerken binnen de Europese Economische Ruimte, tenzij wij hierover met u andere afspraken hebben gemaakt. Deze afspraken leggen wij gezamenlijk schriftelijk vast, of per e-mail. Met ondertekening van deze overeenkomst geeft u toestemming voor de verwerkingen buiten de EER die in de bij deze overeenkomst horende Bijlage worden genoemd.

3.8 A Als wij een verzoek krijgen om persoonsgegevens ter beschikking te stellen dan doen Wij dit alleen als het verzoek is gedaan door een daartoe bevoegde instantie. Bovendien beoordelen wij eerst of wij van mening zijn dat het verzoek bindend is, of dat wij op grond van gedrags- en beroepsregels aan het verzoek moeten voldoen. Als er geen strafrechtelijke of andere juridische belemmeringen zijn, dan stellen wij u op de hoogte van het verzoek. Wij proberen dat op zodanig korte termijn te doen, dat het voor u mogelijk is om eventuele rechtsmiddelen tegen de verstrekking van de persoonsgegevens in te stellen. Als wij u op de hoogte mogen stellen dan zullen Wij ook met u overleggen over de wijze waarop en welke gegevens wij ter beschikking zullen stellen.

4. Beveiligingsmaatregelen

4.1 Wij hebben de beveiligingsmaatregelen genomen die zijn genoemd in de Bijlage die bij deze overeenkomst hoort. Bij het nemen van de beveiligingsmaatregelen is rekening gehouden met de te mitigeren risico's, de stand van de techniek en de kosten van de beveiligingsmaatregelen.

4.2 U heeft zich goed geïnformeerd over de beveiligingsmaatregelen die wij hebben genomen en bent van mening dat deze maatregelen een beveiligingsniveau hebben dat

past bij de aard van de Persoonsgegevens en de omvang, context, doeleinden en risico's van de Verwerking.

4.3 Wij informeren u als een van de beveiligingsmaatregelen substantieel wijzigt.

4.4 Wij bieden passende waarborgen voor de toepassing van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten Verwerkingen. Als u de wijze waarop wij de beveiligingsmaatregelen naleven wilt laten inspecteren, dan kunt u hiertoe een verzoek aan ons doen. Wij zullen hierover gezamenlijk met u afspraken maken. De kosten van een inspectie zijn voor uw rekening. U stelt aan ons een kopie van het inspectierapport ter beschikking.

5. Datalekken

5.1 Als er sprake is van een datalek dan stellen wij u daarvan op de hoogte. Wij streven ernaar dit te doen binnen 24 uur nadat wij dit datalek hebben ontdekt, of zo snel mogelijk nadat wij daarover door onze Sub-verwerkers zijn geïnformeerd. Nadere afspraken over de wijze waarop zijn opgenomen in artikel 11 van deze overeenkomst. Wij zullen u daarbij voorzien van de informatie die u redelijkerwijs nodig heeft om - indien nodig - een juiste en volledige melding te doen aan de Autoriteit Persoonsgegevens en eventueel de betrokkene(n) in het kader van de meldplicht datalekken c.q. wij zenden de melding van onze Sub-verwerker aan u door. Ook van de door ons, of onze Sub-verwerker, naar aanleiding van het datalek genomen maatregelen houden Wij u op de hoogte.

5.2 De melding van datalekken aan de Autoriteit Persoonsgegevens en (eventueel) betrokkene(n) is altijd uw eigen verantwoordelijkheid.

5.3 Het (bij)houden van een register van datalekken is altijd uw eigen verantwoordelijkheid.

Geheimhoudingsplicht

6.1 Wij houden de van u verkregen persoonsgegevens geheim en verplichten onze medewerkers en eventuele Sub-verwerkers ook tot geheimhouding.

7. Aansprakelijkheid

7.1 U staat er voor in dat de verwerking van persoonsgegevens op basis van deze overeenkomst niet onrechtmatig is en geen inbreuk maakt op de rechten van betrokkene(n).

7.2 Wij zijn niet aansprakelijk voor schade die het gevolg is van het door u niet naleven van de AVG of andere wet- of regelgeving. U vrijwaart ons ook voor aanspraken van derden op grond van zulke schade. De vrijwaring geldt niet alleen voor de schade die derden hebben geleden (materieel maar ook immaterieel), maar ook voor de kosten die wij in verband daarmee moeten maken, bijvoorbeeld in een eventuele juridische procedure, en

de kosten van eventuele boetes die aan Ons worden opgelegd ten gevolge van uw handelen.

7.3 De in de onderliggende opdracht en daarbij behorende algemene voorwaarden overeengekomen beperking van onze aansprakelijkheid is van kracht op de verplichtingen zoals opgenomen in deze overeenkomst, met dien verstande dat een of meerdere schadevorderingen uit hoofde van deze overeenkomst en /of de Onderliggende opdracht nimmer tot overschrijding van de beperking kan leiden.

8. Overdraagbaarheid Overeenkomst

8.1 Het is voor u en ons, behalve als wij gezamenlijk schriftelijke anders afspreken, niet toegestaan om deze overeenkomst en de rechten en de plichten die samenhangen met deze overeenkomst over te dragen aan een ander.

9. Beëindiging en teruggave / vernietiging Persoonsgegevens

9.1 Als de onderliggende opdracht wordt beëindigd dan zullen wij de door u aan ons verstrekte persoonsgegevens vernietigen of zo nodig verzamelen en overdragen. Wij zullen uitsluitend een kopie van de persoonsgegevens bewaren als wij hiertoe op grond van wet- of (beroeps)regelgeving verplicht zijn.

9.2 De kosten van het verzamelen en overdragen van persoonsgegevens bij het eindigen van de onderliggende opdracht zijn voor uw rekening. Datzelfde geldt voor de kosten van de vernietiging van de persoonsgegevens. Als u daarom vraagt dan geven wij U vooraf een kosteninschatting.

9.2 Als verwerkingsverantwoordelijke zijn uw medewerkers en uzelf zelf in staat om persoonsgegevens in onze online platforms zelf te vernietigen.

10. Aanvullingen en wijziging Overeenkomst

10.1 Aanvullingen en wijzigingen op deze overeenkomst zijn alleen geldig als ze op schrift zijn gesteld. Onder “schriftelijk” worden ook wijzigingen begrepen die per e-mail zijn gecommuniceerd, gevolgd door een akkoord per e-mail van de andere partij.

10.2 Een wijziging in de verwerkte persoonsgegevens of in de betrouwbaarheidseisen, de privacyregelgeving of uw eisen, kan aanleiding zijn om deze overeenkomst aan te vullen of te wijzigen. Indien dit leidt tot significante aanpassingen in de onderliggende opdracht, of wanneer wij niet kunnen voorzien in een passend niveau van bescherming, kan dit voor ons reden zijn om de onderliggende opdracht te beëindigen.

11. Slotbepalingen

11.1 Op uw verzoek stellen wij u alle informatie ter beschikking die nodig is om de nakoming van de in deze overeenkomst neergelegde verplichtingen aan te tonen. Wij maken audits mogelijk, waaronder inspecties, door u of een door u gemachtigde controleur

en dragen er aan bij. De kosten van dergelijke verzoeken, audits of inspecties zijn voor uw rekening. Ook eventuele audits bij onze sub-verwerkers zijn voor Uw rekening.

11.2 Partijen werken desgevraagd samen met de toezichthoudende autoriteit bij het vervullen van haar taken.

11.3 Op deze overeenkomst is Nederlands recht van toepassing, de Nederlandse rechter is bevoegd kennis te nemen van alle geschillen die voortvloeien uit of samenhangen met deze overeenkomst.

11.4 Deze overeenkomst is hoger in rang dan andere door ons met u gesloten overeenkomsten. Als u algemene voorwaarden gebruikt dan zijn deze niet van toepassing op deze overeenkomst. De bepalingen uit deze overeenkomst gaan boven de bepalingen in onze algemene voorwaarden, tenzij expliciet naar een bepaling in de algemene voorwaarden wordt verwezen.

11.5 Als één of meerdere bepalingen in deze overeenkomst niet geldig blijken te zijn, dan heeft dit geen gevolgen voor de geldigheid van de andere bepalingen in deze overeenkomst. Wij treden dan met u in overleg om gezamenlijk een nieuwe bepaling op te stellen. Deze bepaling zal zoveel als mogelijk in de geest zijn van de ongeldige bepaling, maar dan uiteraard zo vormgegeven dat de bepaling wel geldig is.

11.6 Mededelingen in het kader van deze overeenkomst (inclusief mededelingen in het kader van artikel 5 – datalekken) zullen door u en ons worden gedaan aan onderstaande medewerkers:

[naam]
werkzaam bij: [verwerkingsverantwoordelijke]
[contactgegevens]

[naam]
werkzaam bij: [verwerker]
[contactgegevens]

Als de gegevens behorend bij de bovengenoemde medewerkers veranderen, of als zij worden vervangen door andere medewerkers, dan lichten we elkaar daarover in.

Ondertekening

Ondertekend op .....(datum)

_____	_____
[naam verwerkingsverantwoordelijke + naam ondertekenaar]	Burgerkracht Limburg, dhr. J.H.M von den Hoff Directeur/bestuurder

Bijlage

Persoonsgegevens
De volgende persoonsgegevens worden in het kader van de onderliggende opdracht verwerkt:

- Naam
- Achternaam
- E-mailadres (indien van toepassing)

Sub-verwerkers / Derden
Sub-verwerkers zijn:

- True (IT-voorzieningen)
- Because (salarisadministratie)
- ASP (accountant)
- De Kinderen (verzekeringen)
- Arboned (arbeidsomstandigheden en verzuimbegeleiding)

Technische en organisatorische maatregelen
Wij nemen de volgende technische en organisatorische maatregelen ter bescherming van de Persoonsgegevens tegen verlies of onrechtmatige Verwerking.

Maatregelen tegen inbreuk:

- Geen gebruik cookies
- Encryptie
- Extra versleuteling van database. Database bevat ook alleen betekenisvol de voornaam en achternaam, geslacht en mailadres.
- Toegangslink voor administrators bij de gebruiker is tijdelijk

Maatregelen tegen verlies:

- Back-up procedures: Per uur een back-up en dagelijks een snapshot.

Verwerkingen binnen en buiten de Europese Economische Ruimte
Gegevens worden verwerkt in Nederland en de Europese Economische Ruimte.

Bijlage 4: Minimale en maximale bewaartermijnen

De AVG bepaalt geen concrete bewaartermijn voor persoonsgegevens. Organisaties bepalen zelf hoe lang zij persoonsgegevens bewaren. Van belang is dan hoe lang de gegevens nodig zijn voor het doel waarvoor deze zijn verzameld of worden gebruikt.

De stichting Burgerkracht Limburg hanteert de volgende minimale en maximale bewaartermijnen:

Wat betreft afgesloten bestanden of dossiers, al dan niet geautomatiseerd:
- Individuele personeelsdossiers; 10 jaar na uitdiensttreding na de laatste correspondentie.
- Re-integratietrajecten (WVP) UWV; 10 jaar na uitdiensttreding na de laatste correspondentie.

Wat betreft actieve bestanden of dossiers, al dan niet geautomatiseerd:
- Individuele personeelsdossiers; 10 jaar na uitdiensttreding na de laatste correspondentie m.u.v. medewerkers die in aanraking zijn gekomen met gevaarlijke stoffen.
- Sollicitatiegegevens van niet-benoemde kandidaten en psychologisch onderzoek; uiterlijk 4 weken bij niet-benoemde sollicitanten. Maximaal 1 jaar met schriftelijke toestemming van de kandidaat.
- Psychologisch onderzoek voor bepaling geschiktheid voor functie (benoemde kandidaten; uiterlijk 10 jaar na indiensttreding.
- Rapporten van medische, en andere deskundigen, ook psychologen in het kader van arbeids(on)ge-schiktheid/ stoornissen, verstandelijke beperkingen e.d.; 10 jaar na opmaak rapporten.
- Beoordelingsformulieren; 10 jaar na uitdiensttreding.
- Vertrouwelijke gegevens inzake incidenten behandeld door vertrouwenspersonen en hiervoor benoemde commissies; 10 jaar na datum incident of bij medewerkers 10 jaar na uitdiensttreding.
- Financiële administratiegegevens; 7 jaar.
- Gegevens onroerende zaken; 10 jaar.
- Persoonsgegevens n.a.v. van een bezwaren, klacht- of gerechtelijke procedure; de persoonsgegevens moeten worden verwijderd uiterlijk 1 jaar nadat het bezwaarschrift, de klacht of de gerechtelijke procedure is afgehandeld. Langer bewaren van de gegevens is alleen toegestaan als de persoonsgegevens noodzakelijk zijn ter voldoening aan een wettelijke bewaarplicht.
- Loonbeslagen; tot moment van opheffing.

Er zijn er concrete bewaartermijnen in andere wetten waar Burgerkracht zich uiteraard zal houden.

Bijlage 5 Datalekprotocol

Inleiding

In dit protocol is uitvoering gegeven aan de Algemene Verordening Gegevensbescherming (AVG) EU 2016/679. Deze Verordening is met ingang van 25 mei 2018 van kracht. In de AVG is het begrip “datalek” niet bekend en wordt dit incident een “inbreuk in verband met persoonsgegevens” genoemd; vanwege de bekendheid van het woord ”datalek” wordt in dit protocol dit begrip gebruikt.

Definities

De AVG in artikel 4 lid 1 verstaat onder persoonsgegevens “alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.”
Er is dus sprake van “persoonsgegevens” als die alleen of in samenhang met elkaar kunnen leiden tot identificatie van een levend individu. De AVG is van toepassing als de persoonsgegevens in een bestand zijn opgenomen en als het gegevens betreffen van een zich in de EU bevindende persoon, ongeacht of de verwerking in de EU plaatsheeft. De AVG gaat dus niet over data die niet tot identificatie van een levend individu kunnen leiden.

Onder een inbreuk in verband met persoonsgegevens (art. 4 lid 12 AVG) wordt begrepen “een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde bekendmaking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.”
Er is sprake van een datalek indien persoonsgegevens zich door onvoldoende beveiliging bevinden op een plek waar ze niet thuishoren.
De AVG verplicht EU-organisaties om (art. 32 e.v. AVG) “rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico’s voor de rechten en vrijheden van personen technische en organisatorische maatregelen te treffen om een op het risico afgestemd beveiligingsniveau te waarborgen”.
Gegeven het algemeen behoorlijkheidsbeginsel (art. 5 lid 1 AVG) en het integriteitsbeginsel (art. 5 lid 2 sub f AVG) is het essentieel dat de verwerkingsverantwoordelijke (maar ook de verwerker indien van toepassing) technische en organisatorische beveiligingsmaatregelen neemt ter beveiliging van de aan haar toevertrouwde persoonsgegevens. De organisatie is tevens verplicht om de toezichthouder (i.c. in Nederland de Autoriteit Persoonsgegevens (AP)) te informeren over inbreuken op de beveiliging (art. 33 AVG) en onder omstandigheden ook de betrokkenen (art. 34 AVG).

Toepasselijkheid datalekbepalingen

De stichting Burgerkracht Limburg (hierna Burgerkracht Limburg) is een organisatie die volledig aan de bovengenoemde verplichtingen dient te voldoen.

Voor dit protocol wordt ervan uitgegaan dat Burgerkracht Limburg (overwegend) de rol van “verwerkingsverantwoordelijke” heeft omdat deze, al dan niet in samenwerking met anderen, het doel en de middelen (om dat doel te bereiken) voor de verwerking van persoonsgegevens vaststelt. Mogelijk kent Burgerkracht Limburg bij sommige verwerkingen de rol van “verwerker”. Het stappenplan in dit protocol verandert daardoor niet, alleen geldt de meldplicht dan in die situatie aan de “verwerkingsverantwoordelijke” in plaats van aan de Autoriteit Persoonsgegevens.

Melding datalek

De melding van een datalek is omschreven in artikel 33 van de AVG. Burgerkracht Limburg meldt een datalek zonder onnodige vertraging en - indien mogelijk - binnen 72 uur na constatering van de inbreuk bij de Autoriteit Persoonsgegevens (hierna de AP) tenzij “het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen”. Hoewel datalekken altijd vermeld dienen te worden in het privacy-dossier, kan een melding aan de AP (en dus ook aan de betrokkenen) achterwege blijven als de inbreuk redelijkerwijs geen risico voor betrokkene(-n) inhoudt.
De melding aan de AP gebeurt via de link https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0 die leidt naar het meldloket datalekken.
Art. 34 van de AVG vermeldt het volgende: “Indien de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de betrokkenen de inbreuk in verband met persoonsgegevens onverwijld mee na ontdekking hiervan.” Voorbeelden van een hoog risico zijn het verlies van controle over hun persoonsgegevens waardoor identiteitsfraude tot de mogelijkheden behoort, het niet kunnen uitoefenen van hun rechten, kans op discriminatie, financiële verliezen en reputatieschade.

Rolverdeling melden datalek

Binnen Burgerkracht worden de volgende rollen uitgevoerd:
Privacy-officer. Deze functionaris is de centrale figuur in de vermijding en bestrijding van datalekken. Hij is verantwoordelijk voor de eerste beoordeling van de ernst van de (vermoedelijke) inbreuk en voor de uitvoering van de melding aan AP en betrokkene(-n). Hij communiceert intern met de IT verantwoordelijke, het privacy-team en de verantwoordelijke bestuurder, aan welke laatste hij per kwartaal verslag doet van alle voor de naleving van de AVG relevante gebeurtenissen. In overleg met dezen bepaalt hij de wijze waarop de betrokkene(-n) in kennis worden gesteld van de inbreuk en de tekst van de boodschap waarin onder meer aangegeven wordt hoe de betrokkene(-n) de gevolgen van het incident kan (kunnen) mitigeren. Hij is de eerste contactpersoon voor AP en stakeholders inzake de uitvoering van de bepalingen in de AVG bij Burgerkracht hij is bevoegd de melding aan de AP te verrichten.
IT-verantwoordelijke. Deze functionaris is verantwoordelijk voor en volledig op de hoogte van bij Burgerkracht toegepaste hardware en software, het gebruik daarvan en de bescherming van de gegevens op deze systemen, zowel technisch als organisatorisch. Hij adviseert over en controleert het vastgestelde beleid ten aanzien van onder andere het gebruik van wachtwoorden en andere verificatiemogelijkheden, blokkering van accounts,

tijdelijk stopzetten van diensten, gebruik van wifi en regels omtrent thuiswerken van medewerkers, et cetera. De IT-verantwoordelijke is dhr. Carel Berkhoff.
Bestuurder. Deze functionaris is eindverantwoordelijke voor de AVG en de contacten met de AP en ontvangt zonder onnodige vertraging alle relevante informatie omtrent (mogelijke) datalekken. Als eindverantwoordelijke besluit hij of zij over de adviezen die hij of zij van de privacy-officer, de IT-verantwoordelijke en/of het privacy-team ontvangt.
Privacy-team. Het privacy-team vormt een afspiegeling van de organisatie en omvat behalve de privacy-officer, de IT-verantwoordelijke en in ieder geval de HR manager en de controller.

Uit te voeren stappen bij een datalek

De volgende opvolgende stappen zijn in het proces van omgaan met een (mogelijk) datalek van toepassing en worden hierna per stap toegelicht:

- Ontdekking van een mogelijke inbreuk.
- Interne melding van de mogelijke inbreuk.
- Beoordeling van de ernst van de gemelde inbreuk, zowel voor Burgerkracht als voor de betrokkene(-n).
- Response door de IT-verantwoordelijke en indien nodig bestrijding van het lek.
- Response door de privacy-officer en indien nodig melding van de inbreuk aan AP.
- Response door de privacy-officer en indien nodig melding van de inbreuk aan de betrokkene(-n).
- Response door de privacy-officer en indien nodig of gewenst melding aan overige stakeholders.
- Bepaling van de acties voor verbetering van de beveiliging, zowel technisch als organisatorisch.
- Regelen van de nazorg aan de betrokkene(-n).
- Registreren, evalueren en verbeteren.

Ontdekking van een mogelijke inbreuk en interne melding

Burgerkracht instrueert de medewerkers dat ALLE signalen die kunnen wijzen op een datalek gemeld dienen te worden aan de privacy-officer.

Beoordeling van de ernst van de gemelde inbreuk

De privacy-officer gaat in overleg met de melder van het incident en bouwt zich daarmee een beeld op van het betreffende incident aan de hand van de volgende vragen:

- Waar heeft het incident plaatsgevonden?
- Welke systemen zijn daarbij betrokken?
- Indien van toepassing: waar heeft het verlies of de diefstal van fysieke gegevensdragers plaatsgevonden en onder welke omstandigheden?
- Om welke data handelt het (AVG meldplicht is alleen van toepassing op persoonsgegevens)?
- Om welke persoonsgegevens gaat het en om hoeveel personen?
- Is er mogelijk sprake van schending van vertrouwelijkheid, beschikbaarheid en/of van integriteit van de persoonsgegevens?

- Welke bedrijfsprocessen kunnen verstoord raken door het incident?
- Wat is de vermoedelijke oorzaak?
- Is het datalek voorbij of is de verwachting dat het systeem verder geïnfiltreerd kan worden?

De privacy-officer maakt verslag van de antwoorden en gaat in overleg met de IT verantwoordelijke over de aan de eindverantwoordelijke bestuurder te adviseren te nemen maatregelen.

Response door de IT verantwoordelijke en bestrijding van het lek.

De IT verantwoordelijke bepaalt op basis van de door de privacy-officer aan hem verstrekte informatie de acties die onmiddellijk genomen moeten worden om verder lekken te voorkomen en de geconstateerde onvolkomenheden in het systeem te verhelpen. Hij heeft daarbij de volgende bevoegdheden:

- Tijdelijk blokkeren van accounts.
- Aanpassen van de firewall configuraties.
- Wijzigen van wachtwoorden.
- Verzamelen van bewijsmateriaal om de veroorzaker aan te kunnen wijzen en aan te kunnen blokkeren.
- Op afstand wissen van bestanden op geïnfecteerde devices.

Response door de privacy-officer en indien nodig melding van de inbreuk aan de AP

Indien de conclusie uit de beoordeling van de ernst van de gemelde inbreuk is dat er waarschijnlijk sprake is van een risico voor de rechten en vrijheden van de betrokkene(-n) doet de privacy-officer binnen 72 uur na constatering van de inbreuk melding hiervan aan de AP via de link https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0 Hieronder verschijnt een pagina met de button “nieuwe melding” waarna een vragenlijst volgt die geheel beantwoord dient te worden door degene die daartoe bevoegd is (i.c. de privacy-officer). Indien zij dat nodig of gewenst acht, kan de privacy-officer advies over de te geven antwoorden inroepen van een externe deskundige.

Response door de privacy-officer en indien nodig melding van de inbreuk aan de betrokkene(-n)

Bij een hoog risico voor de betrokkene(-n) dienen deze van de inbreuk op de hoogte te worden gesteld. De privacy-officer bepaalt de hoogte van het risico door een inschatting te maken van de kans op nadelige gevolgen voor de betrokkene(-n) en de mate van ernst voor de gevolgen van de inbreuk voor de betrokkene(-n). De privacy-officer bepaalt welke vorm van communicatie met de betrokkene(-n) het meest geschikt is om de schade voor de betrokkene(-n) zoveel mogelijk te beperken. De mededeling aan betrokkene(-n) bevat tenminste:

- een omschrijving van het feit in duidelijke en eenvoudige taal;
- de naam en contactgegevens van de privacy-officer;
- de waarschijnlijke gevolgen van de inbreuk;
- de maatregelen die Burgerkracht genomen heeft om de nadelige gevolgen voor de betrokkene(-n) te beperken;

- de maatregelen die de betrokkene(-n) zelf moet(-en) nemen om die gevolgen te beperken en herhaling te voorkomen.

Response door de privacy-officer en indien nodig of gewenst melding aan overige stakeholders

Bij zeer ernstige datalekken of om andere haar moverende redenen kan de privacy-officer na overleg met de bestuurder besluiten om bepaalde stakeholders te informeren over de inbreuk. De partijen die hiervoor in aanmerking kunnen komen zijn de aandeelhouders en andere kapitaalverschaffers, het personeel, leveranciers, media, verzekeraars, et cetera.

Bepaling van de acties voor verbetering van de beveiliging, zowel technisch als organisatorisch

Datalekken zijn altijd een gevolg van onvoldoende beveiliging van de gegevens op een bepaald moment. Burgerkracht tracht steeds te voldoen aan een adequate beveiliging conform artikel 32 van de AVG waarin sprake is van “passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen” zulks “rekening houdend met de stand van de techniek en de uitvoeringskosten” en het risico voor de betrokkene(-n). Dit betekent een vergaande inspanningsverplichting om de beveiligingsmaatregelen op een passend niveau te brengen. Bij de bepaling van de acties voor verbetering houdt de IT verantwoordelijke onder meer rekening met:

- mogelijkheden voor pseudonimisering en encryptie van persoonsgegevens;
- de mogelijkheden om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en de veerkracht van de verwerkingssystemen te garanderen;
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid en de toegang tot de persoonsgegevens tijdig te herstellen (PDCA cyclus);
- een procedure om voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de genomen maatregelen;
- regelmatige scholing en instructie van personeel van Burgerkracht waardoor datalekken door menselijk falen tot een minimum worden teruggebracht.

Regelen van de nazorg aan de betrokkene(-n)
Rekening houdende met de ernst van de gevolgen van de inbreuk voor de betrokkene(-n) bepaalt de privacy-officer in overleg met de bestuurder en het privacy-team welke additionele acties gewenst zijn om het eventueel geschonden vertrouwen in Burgerkracht te herstellen en de reputatieschade te beperken.

Registreren, evalueren en verbeteren
De privacy-officer registreert elk incident, ook als dit geen datalek blijkt te zijn en dus niet gemeld hoeft te worden. Deze registratie stelt Burgerkracht in staat om structureel aan verbetering te werken. De registratie vindt plaats in een daarvoor gereserveerd hoofdstuk in het privacy-dossier van Burgerkracht. Het privacy-team evalueert op jaarbasis de geregistreerde incidenten en doet voorstellen voor verbetering.
Voor wijzigingen in de zienswijze, voor richtsnoeren, publicaties en voor toelichtingen op het melden van datalekken volgt de privacy-officer de meldingen van de Autoriteit

Persoonsgegevens middels publicaties op hun site www.autoriteitpersoonsgegevens.nl en middels een abonnement op de nieuwsbrief van deze autoriteit.

Meldingsformulier Datalekken
Burgerkracht verplicht alle medewerkers om een geconstateerde inbreuk op de beveiliging van de persoonsgegevens bij Burgerkracht binnen 24 uur na vaststelling te melden via dit formulier.

- Gegevens melder

- Naam
- Telefoonnummer
- E-mailadres
- Functie
- Beschrijving incident

Beschrijf zo volledig mogelijk de oorzaak en het (mogelijke) resultaat van de inbreuk op de beveiliging van persoonsgegevens

- Wanneer is de inbreuk geconstateerd?

- Datum:
- Tijdstip:
- Wanneer vond de inbreuk plaats?
- Datum:
- Tijd of tijdvak/periode:

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

Klanten / medewerkers / anders, namelijk

- Wat is de aard van de inbreuk?

Lezen / Kopiëren / Veranderen / Verwijderen of vernietigen / Diefstal / Verlies /Anders, namelijk:

Van hoeveel personen zijn de persoonsgegevens betrokken bij de inbreuk?

Minimaal:

Maximaal:

Om welke typen persoonsgegevens gaat het bij de inbreuk?
Kruis aan indien van toepassing:
0 naam-, adres- en woonplaatsgegevens
0 telefoonnummers
0 e-mailadressen of andere adressen voor elektronische communicatie
0 toegangs- of identificatiegegevens (bijvoorbeeld inlognaam/wachtwoord of klantnummer)
0 financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)
0 BSN- of sofinummer
0 paspoort kopieën of kopieën van andere legitimatiebewijzen
0 geslacht, geboortedatum en/of leeftijd
0 bijzondere gegevens (zoals medische gegevens etc.)
0 overige, namelijk

Waren de persoonsgegevens versleuteld, gehasht of op een andere manier beveiligd?
Als de gegevens beveiligd waren, geef dan aan hoe dit is gebeurd.
Beschrijving:

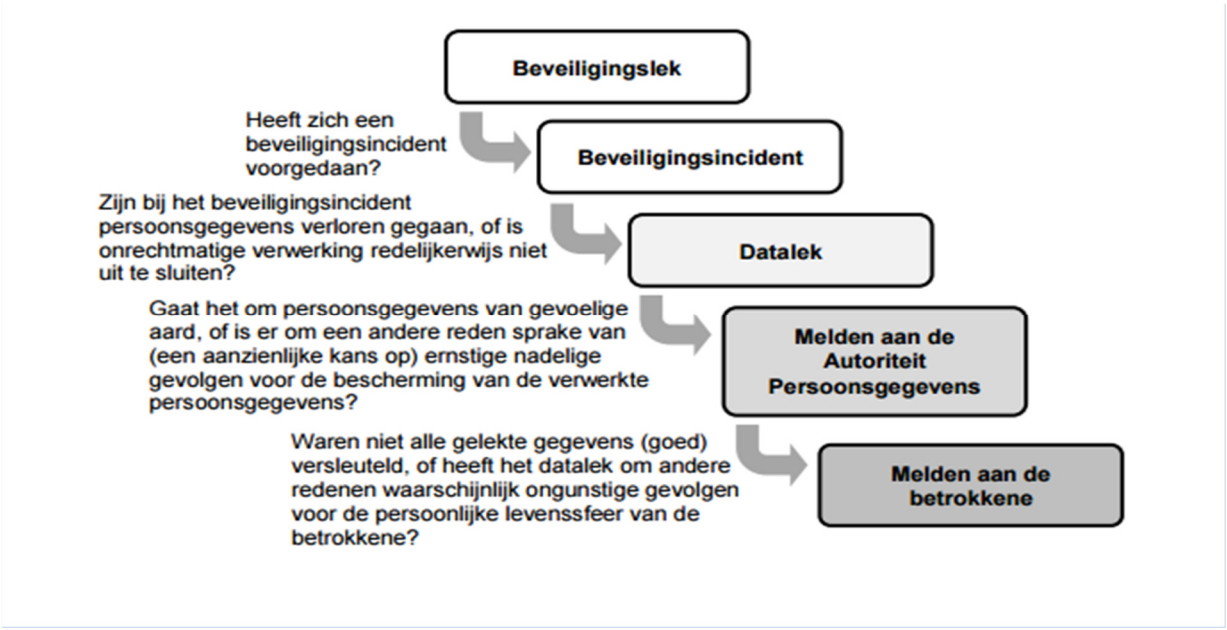
Heeft de inbreuk (ook) betrekking op personen in andere EU-landen naast Nederland?
Ja / Nee / Niet bekend

Welke technische en/of organisatorische maatregelen heeft u of het bedrijf getroffen?
Beschrijf welke maatregelen u of uw bedrijf heeft getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen.

- Beschrijf:
- Ondertekening
- Melder Functionaris voor de gegevensbescherming
- Datum

Samenvatting melding datalek

Onderstaand een schematische voorstelling voor instructiedoeleinden van de melding van een datalek:


Beveiligingslek
Heeft zich een beveiligingsincident voorgedaan?
Beveiligingsincident
Zijn bij het beveiligingsincident persoonsgegevens verloren gegaan, of is onrechtmatige verwerking redelijkerwijs niet uit te sluiten?
Datalek
Gaat het om persoonsgegevens van gevoelige aard, of is er om een andere reden sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens?
Melden aan de Autoriteit Persoonsgegevens
Waren niet alle gelekte gegevens (goed) versleuteld, of heeft het datalek om andere redenen waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene?
Melden aan de betrokkene