Beleid

Gegevensverwerking binnen G4S België

Securing Your World

Inhoudstafel

1. Inleiding

Het Europees Parlement heeft op 14 april 2016 verordening (EU) 2016/679 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG aangenomen. Deze verordening is beter bekend onder de naam *General Data Protection Regulation* (GDPR)[1].

Dit document is gebaseerd op de GDPR en geeft algemene beleidsuitgangspunten over privacy binnen G4S België[2] weer. Met privacy wordt verwezen naar de bescherming van persoonsgegevens. Verwerking van persoonsgegevens is noodzakelijk voor de bedrijfsprocessen binnen G4S alsmede de processen die G4S heeft uitbesteed aan derde partijen. Dit dient met een bepaald doel, subsidiair, proportioneel en zorgvuldig te gebeuren omdat verkeerd behandelen van persoonsgegevens kan leiden tot grote schade voor klanten, leveranciers, medewerkers, andere betrokkenen en G4S zelf. G4S hecht dan ook veel waarde aan het zo juist mogelijk beschermen van persoonsgegevens die aan haar worden verstrekt en de manier waarop deze gegevens worden verwerkt. De verantwoordelijkheid voor de bescherming van persoonsgegevens ligt bij de directie van G4S.

Met het beschrijven van maatregelen in dit beleidsdocument neemt G4S haar verantwoordelijkheid om de kwaliteit van de beveiliging van de persoonsgegevens te optimaliseren.

1.1 Persoonsgegevens, data en informatie

Bescherming van persoonsgegevens (privacy), data en informatie zijn verweven met elkaar, echter is er wel een onderscheid tussen de begrippen. Privacy is het recht om meester over de eigen persoonsgegevens te zijn. Data zijn een hoeveelheid gegevens. Informatie wordt gezien als gegevens die een bepaalde betekenis krijgen. Kortom, data heeft men nodig om informatie te krijgen en de data moet worden beschermd zodat de persoonsgegevens van de betrokkenen, en dus hun privacy niet, of zo min mogelijk, wordt geschonden.

1.2 Scope en doelstellingen van het beleid

Dit beleid heeft betrekking op de verwerking van persoonsgegevens onder verantwoordelijkheid van G4S. Het heeft zowel betrekking op interne bedrijfsprocessen als op processen die zijn uitbesteed aan derden. G4S dient voor haar bedrijfsdoeleinden bepaalde informatie over personen te verzamelen en te gebruiken. Dit kunnen klanten, leveranciers, zakencontacten, werknemers of andere mensen zijn.

[1] In dit document wordt de term GDPR gehanteerd.
[2] Hierna G4S genoemd. Huidig beleidsdocument is van toepassing op G4S SECURE SOLUTIONS NV en haar verbonden vennootschappen of personen bedoeld zoals bepaald in artikel 11 van het wetboek van vennootschappen.

Het beleid is van toepassing op geheel of gedeeltelijk geautomatiseerde/systematische verwerking van persoonsgegevens evenals op niet-geautomatiseerde verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van G4S.

G4S interpreteert het beschermen van persoonsgegevens breed. Zo is er een relatie en gedeeltelijke overlap met informatiebeveiliging. Informatiebeveiliging is de verzamelnaam voor processen die erop gericht zijn de betrouwbaarheid van alle vormen van informatie binnen een organisatie te garanderen. De betrouwbaarheid wordt bepaald door te monitoren op:

- Beschikbaarheid: zorg dragen voor de beschikbaarheid van informatie en informatie verwerkende bedrijfsmiddelen op de juiste plaats en tijd voor gebruikers.
- Integriteit: waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van de informatie en de verwerking daarvan.
- Vertrouwelijkheid: beschermen van informatie tegen verwerkingen door onbevoegden.

Informatiebeveiliging heeft als doel de continuïteit van informatie te waarborgen en de gevolgen van beveiligingsincidenten tot een vooraf bepaald acceptabel niveau te beperken, maar ook om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren waarbij een gezonde en goede balans moet worden gevonden tussen veiligheid, privacy en functionaliteit.

G4S respecteert de persoonlijke levenssfeer van betrokkenen. Persoonsgegevens dienen adequaat beschermd te worden tegen inbreuken, al dan niet onrechtmatig. Dit brengt met zich mee dat G4S dient te voldoen aan relevante wet- en regelgeving met betrekking tot de verwerking van persoonsgegevens.

De doelstellingen van dit beleid zijn als volgt:

- Het stellen van normen: de basis voor de beveiliging van persoonsgegevens is de G4S Group Information Security Mandatory Minimal Security Controls (MMSC)[3] Implementation Standard en best practices vanuit de Veiligheidsbranche.
- Het bieden van een kader: het beleid biedt een kader om verwerkingen (ook toekomstige) van persoonsgegevens te toetsen aan een norm of een overeengekomen ‘best practice’.
- Taken, bevoegdheden en verantwoordelijkheden in de organisatie te beleggen.
- Het nemen van verantwoordelijkheid: de directie dient de uitgangspunten en de organisatie voor het verwerken van persoonsgegevens vast te leggen voor geheel G4S en dit uit te dragen.
- Als marktleider een voorbeeld te zijn voor andere beveiligingsorganisaties.
- Implementatie van het beleid door duidelijk keuzes in maatregelen te maken en actieve controle toe te passen op de uitvoering van beleidsmaatregelen.

[3] De MMSC is de standaard voor informatiebeveiliging die G4S hanteert en is een afgeleide van ISO 27001; de internationale standaard voor informatiebeveiliging.

- Creëren van bewustwording van het belang en noodzaak om persoonsgegevens te beschermen bij de (externe) medewerkers van G4S.
- Compliant zijn met de Belgische en Europese wetgeving.

1.3 Definities

Alle in dit document gehanteerde specifieke begrippen hebben de betekenis die zij in de GDPR gekregen hebben. Begrippen die niet in de GDPR gedefinieerd werden, dragen hun algemeen taalkundige betekenis. Onderstaande begrippen krijgen de volgende betekenis:

- Privacy by default: instellingen van een product of dienst standaard op de meest privacy vriendelijke stand te zetten.

- Privacy by design: aandacht voor privacy gedurende de gehele levenscyclus van een systeem, vanaf het ontwerpen tot aan het verwijderen van het systeem.

1.4 Opbouw document

Achtereenvolgend komen de volgende onderwerpen ter sprake: principes verwerking persoonsgegevens, organisatie met betrekking tot verwerking persoonsgegevens, implementatie van het beleid, behoorlijke en zorgvuldige verwerking van persoonsgegevens, incidenten, rechten van betrokkene en beheer van het document.

2. Principes verwerking persoonsgegevens

Uitgangspunt voor het beleid is dat persoonsgegevens in overeenstemming met de huidige vigerende wet- en regelgeving op zorgvuldige en behoorlijke wijze worden verwerkt. Een goede balans moet worden gevonden tussen het belang van G4S om persoonsgegevens te verwerken en het belang van de betrokkene om eigen keuzes te maken met betrekking tot zijn of haar gegevens.

De volgende principes zijn opgesteld om aan het uitgangspunt te voldoen:

- Elke verwerking van persoonsgegevens is gebaseerd op één van de wettelijke grondslagen zoals genoemd in de GDPR.
- Persoonsgegevens worden alleen verwerkt voor duidelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking geformuleerd.
- Bij een verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt tot de persoonsgegevens die noodzakelijk zijn voor het specifieke doeleinde. De gegevens dienen met het oog op dat doel toereikend, relevant en niet bovenmatig te zijn.
- Verwerking van persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde.
- Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken persoonsgegevens correct en up-to-date zijn.
- Persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen.
- Persoonsgegevens worden niet langer verwerkt dan noodzakelijk is voor de doeleinden van de verwerking, hierbij worden de van toepassing zijnde bewaar- en vernietigingstermijnen in acht genomen.
- Er wordt een register van verwerkingsactiviteiten opgesteld.
- Privacy by design en privacy by default worden gehanteerd.
- Iedere betrokkene heeft recht op inzage respectievelijk rectificatie, gegevenswissing, beperking van de verwerking en overdraagbaarheid, zoals geformuleerd in hoofdstuk 7 van dit beleid.

3. Organisatie met betrekking tot verwerking persoonsgegevens

G4S België heeft een GDPR Project Team onder leiding van de Projectleider (Manager Public & Legal Affairs). Uiterlijk op 25 mei 2018 zal G4S een Data Protection Officer (ook Data Officer of Privacy Officer genoemd) aanstellen. Tot dan vallen de taken & verantwoordelijkheden van de Data Protection Officer onder de bevoegdheid van de Projectleider. Alle G4S België Business Units (BU's) zijn vertegenwoordigd in het GDPR Project Team.

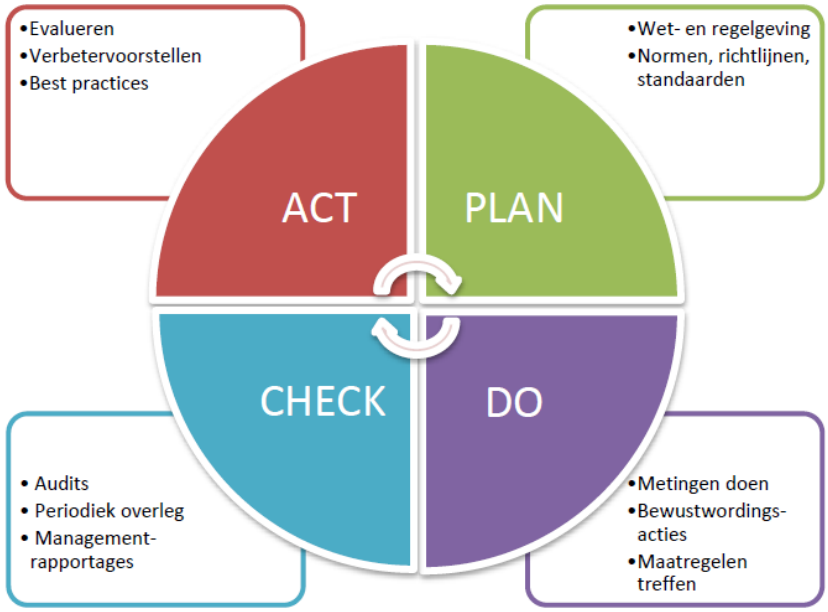
4. Implementatie van het beleid

De directie van G4S is eindverantwoordelijke voor de verwerking van persoonsgegevens. Echter wordt de feitelijke verwerking binnen verschillende entiteiten van G4S uitgevoerd. In dit hoofdstuk wordt beschreven hoe het beleid wordt geïmplementeerd.

4.1 Plan, Do, Check, Act-cyclus

Het borgen van privacy is een continu kwaliteitsproces. Plan, Do, Check, Act (PDCA) vormen gezamenlijk het managementsysteem van privacy. Deze kwaliteitscyclus is in Figuur 1 weergegeven.

Figuur 1 PDCA-cyclus



Toelichting op de PDCA-cyclus:

- Plan: De cyclus start met het opstellen van een beleid. Dit beleid is gebaseerd op de wet- en regelgeving, normen vanuit de branche. Daarnaast worden richtlijnen en standaarden opgesteld. Het beleid wordt elk jaar herzien en indien nodig tussentijds bijgesteld.
- Do: het beleid vormt de basis om bewustwordingsacties op te zetten, metingen te verrichten in de organisatie en om maatregelen te treffen. Uitvoering van deze acties maakt onderdeel uit van het dagelijks werkproces. Beleid wordt vertaald naar concrete plannen.
- Check: controle van naleving van het beleid gebeurt door het doen van audits binnen de organisatie en door het voeren van periodiek overleg met interne stakeholders. Doel van controle is om de bescherming van persoonsgegevens te borgen en

compliant te zijn aan de wet- en regelgeving. De bevindingen uit de audits worden gerapporteerd aan de desbetreffende afdeling/BU's en indien noodzakelijk aan de directie. Daarnaast worden periodiek managementrapportages opgesteld.

- Act: op basis van audits en overleggen worden processen geëvalueerd en verbetervoorstellen voorgesteld en mogelijk best practices ontwikkeld. Indien sprake is van ingrijpende verbetervoorstellen dan wordt dit als een beslissing voorgelegd aan de directie.

4.2 Verdeling van de verantwoordelijkheden

De verwerking van persoonsgegevens dient te worden gezien als een gedelegeerde verantwoordelijkheid vanuit de directie naar de verschillende BU's. De managers en directeurs zijn primair verantwoordelijk voor een zorgvuldige verwerking van persoonsgegevens binnen hun bedrijfsprocessen. Dit omvat ook het invoeren van de maatregelen, uitvoering en handhaving daarvan. Daarnaast is het een taak van de managers en directeuren om dit beleid met alle relevante partijen te bespreken.

Zorgvuldig omgaan met persoonsgegevens is een verantwoordelijk van iedere medewerker van G4S. Onder zorgvuldig omgaan met persoonsgegevens wordt onder andere verstaan:

- Hanteren van clean desk/clean screen;
- Geen bedrijfsgoederen met data in de auto laten liggen;
- Gebruik maken van de papierbak en deze legen in de beveiligde papiercontainer;
- Signaleren en proactief melden van risico's met betrekking tot privacy aan de leidinggevende;
- Et cetera.

Van medewerkers wordt verwacht dat zij zich integer gedragen met betrekking tot verwerking van persoonsgegevens. Het is ontoelaatbaar dat door al dan niet opzettelijk gedrag situaties ontstaan die kunnen leiden tot schade of reputatieverlies van G4S of van betrokkenen. Om deze reden zijn gedragscodes opgesteld en geïmplementeerd en wordt continu aandacht besteed aan awareness.

5. Behoorlijke en zorgvuldige verwerking van persoonsgegevens

5.1 Verwerkingen

Het verwerken van persoonsgegevens dient gebaseerd te zijn op een van de wettelijke gronden zoals omschreven in de GDPR. De wettelijke gronden zijn als volgt:

a) Betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
b) Verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene voor de sluiting van een overeenkomst maatregelen te nemen;
c) Verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
d) De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
e) De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
f) De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanner de belangen of grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.
g) Iedere mogelijke toekomstige uitbreiding van de wettelijke gronden bepaald in de GDPR.

De verantwoordelijke van het bedrijfsproces omschrijft vooraf de doeleinden voor de verwerking. Elke verwerking wordt gemeld bij de privacy officer. De privacy officer toetst vervolgens of de verwerking noodzakelijk is en of de doeleinden rechtsgeldig zijn. De privacy officer houdt conform de GDPR een register van verwerkingsactiviteiten bij.

Systemen waarin persoonsgegevens worden verwerkt, dienen te voldoen aan de eisen uit de Mandatory Minimum Security Controls (MMSC). Bij infrastructurele wijzigingen of de aanschaf van nieuwe systemen wordt van tevoren een Privacy Impact Assessment (PIA) uitgevoerd (hieronder volgt meer). Daarnaast worden de principes van privacy by design en privacy by default, zoals in de GDPR beschreven, gehanteerd.

Bijzondere persoonsgegevens[4] worden niet verwerkt, tenzij dit nodig is voor het uitvoeren van een wettelijke taak of regeling. Indien bijzondere persoonsgegevens worden verwerkt, dan zijn deze gescheiden en worden deze zwaarder beveiligd dan andere persoonsgegevens.

5.2 Bescherming van gegevens

G4S treft passende organisatorische en technische maatregelen ter bescherming en bevordering van de beschikbaarheid, integriteit en vertrouwelijkheid van persoonsgegevens en ter voorkoming van verlies, inbreuk en onrechtmatige verwerking van persoonsgegevens. Naast het hanteren van de MMSC standaard zijn er meerdere manieren om gegevensbescherming te borgen, zoals het uitvoeren van een PIA, classificeren van data en logging van gegevensgebruik.

5.2.1. Privacy Impact Assessment (PIA)

Het uitvoeren van een PIA is een manier om gegevensbescherming te borgen. Een PIA geeft de privacyrisico's weer van bestaande en nieuwe verwerkingen van gegevens. Op basis daarvan kunnen maatregelen worden getroffen. Conform de GDPR dient een PIA te worden uitgevoerd in de volgende situaties:[5]

- Als sprake is van beoordeling op systematische en uitvoerig persoonlijke aspecten, waaronder profiling;
- Op grote schaal bijzondere persoonsgegevens worden verwerkt;
- Als men op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht).

5.2.2. Dataclassificatie

Elk systeem waarin persoonsgegevens worden verwerkt is anders en dient op maat te worden geclassificeerd. Dataclassificatie heeft als doel om de beschikbaarheid, integriteit en vertrouwelijkheid van het systeem vast te stellen. Dit maakt duidelijk welke maatregelen nodig zijn om het betreffende systeem te beschermen.

5.2.3. Logging van gegevensgebruik

Elk geautomatiseerd systeem dat persoonsgegevens verwerkt, moet logging bijhouden van de verwerkingen. De volgende zaken moeten minimaal worden geregistreerd: welke gebruiker, welk tijdstip en wat er wordt verwerkt.

[4] Bijzondere persoonsgegevens zijn conform artikel 9 GDPR: ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap vakbond, genetische- en biometrische gegevens, gegevens over gezondheid, gegevens met betrekking tot seksueel gedrag/seksuele geaardheid en alle mogelijke toekomstige uitbreidingen van dit begrip.

[5] Op termijn publiceert de Toezichthoudende Autoriteit een lijst van verwerkingen waarvoor een PIA verplicht is. Deze lijst is nog niet bekend bij de opmaak van dit document, maar is er integraal op van toepassing.

5.2.4. Bewaartermijnen

Persoonsgegevens mogen niet langer worden bewaard dan vereist voor het doel waarvoor zij gebruikt of verzameld werden. Bewaartermijnen kunnen wettelijk of door G4S worden vastgesteld. Persoonsgegevens dienen vernietigd te worden zodra de bewaartermijn is verstreken.

Indien persoonsgegevens bestemd zijn voor historische, statistische of wetenschappelijke doeleinden dan dienen deze gegevens te worden bewaard in een apart archief en ook op deze manier benoemd te worden.

5.3 Verwerkersovereenkomst

G4S besteedt processen en diensten uit aan derden. Het uitbesteden van processen en diensten brengt risico's met zich mee met betrekking tot gegevensverwerking en informatiebeveiliging. G4S blijft verantwoordelijk voor de verwerking van die gegevens. Om de verantwoordelijkheid te kunnen managen wordt bij elke uitbesteding waarbij persoonsgegevens in het spel zijn een verwerkersovereenkomst afgesloten.

De privacy officer is eigenaar van de overeenkomst en past deze aan indien nodig. Het is de verantwoordelijkheid van de manager van de afdeling of de directeur van een BU om deze overeenkomsten af te sluiten en te beheren. De privacy officer controleert of dit wordt nageleefd en geeft advies.

6. Incidenten

6.1 Beveiligingsincidenten en datalekken

Incidenten kunnen voorkomen en daar dient adequaat op te worden gereageerd. Er kan sprake zijn van een beveiligingsincident of een datalek. Een beveiligingsincident is een gebeurtenis waardoor mogelijk afbreuk is gedaan aan de integriteit, vertrouwelijkheid of beschikbaarheid van gegevens.[6] Een datalek is toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie, al dan niet onrechtmatig.[7] Bij een datalek is het zeker dat persoonsgegevens verloren zijn gegaan of dat onrechtmatige verwerking niet kan worden uitgesloten.[8]

6.2 Melding en registratie

Beveiligingsincidenten en datalekken dienen gemeld te worden via de Privacy Meldlijn (02/507.20.46) van de alarmcentrale of via de ICT-servicedesk (privacy.leak@be.g4s.com). Elk incident wordt geregistreerd. De bewaartermijn voor een incident is drie jaar.

De Privacy Meldlijn en het Privacy Mailadres zijn bestemd zowel voor interne medewerkers als voor externe stakeholders.

Conform de GDPR dient G4S binnen 72 uur een melding te doen bij de Toezichthoudende Autoriteit (TA) als er sprake is van een datalek. De melding aan de TA kan en mag uitsluitend door de privacy officer worden gedaan.

Conform de GDPR dient G4S de betrokkenen te informeren over het datalek. Dit dient te gebeuren indien het datalek ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene.[9]

Elke twee maanden bezorgt de privacy officer een update over de incidenten die hebben plaatsgevonden aan de directie. Daarnaast stelt de privacy officer een jaarrapportage op.

6.3 Privacyteam

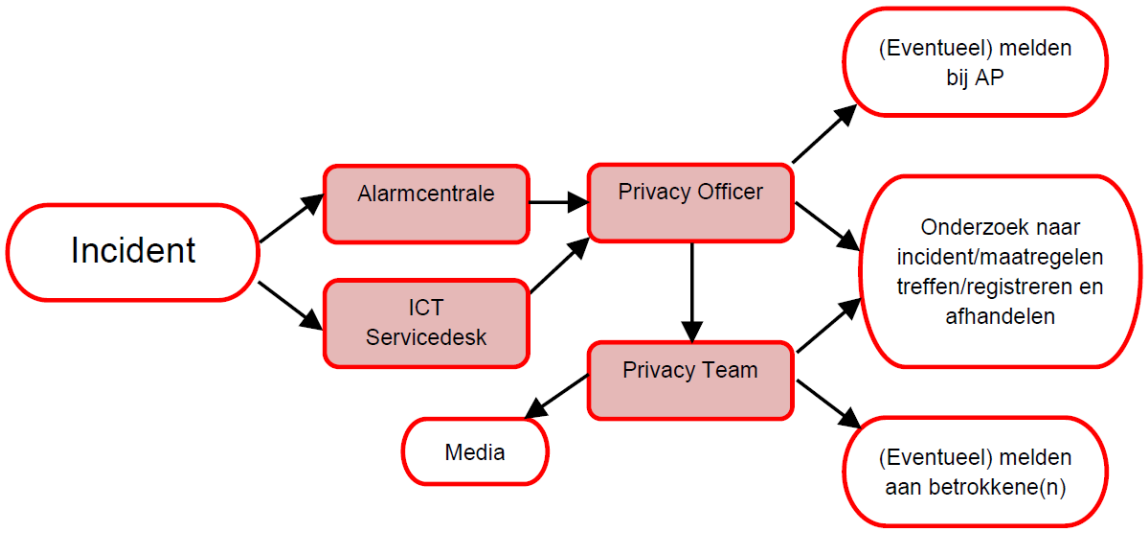
De privacy officer beoordeelt het incident en bepaalt in eerste instantie of het gaat om een beveiligingsincident of een datalek en of de betrokkenen moeten worden geïnformeerd. De beoordeling wordt vervolgens gedeeld met het privacyteam om te bepalen wat het definitieve oordeel wordt. In het privacy team zitten naast de Privacy Officer in ieder geval de manager Legal & Public Affairs en de Managing Director. Het besluit om een incident wel of niet te melden bij de TA gebeurt altijd in overleg met de directie.

[6] Een voorbeeld van een beveiligingsincident is de diefstal van een laptop.
[7] Een voorbeeld van een datalek is de diefstal van een laptop met onversleutelde, financiële klantgegevens.
[8] Een datalek is altijd een beveiligingsincident. Een beveiligingsincident hoeft niet altijd een datalek te zijn.
[9] Een voorbeeld van een situatie waarbij de betrokkene geïnformeerd dient te worden is de situatie waarbij wachtwoorden en gebruikersnamen zijn gelekt.

Per incident wordt het privacyteam aangevuld met de manager/directeur van het betrokken bedrijfsproces en een lid van de IT-afdeling. Het privacyteam anticipeert op een eventuele reactie in de media.

Het proces van melding tot afhandeling is weergegeven in onderstaande figuur.

Figuur 2 proces melding – afhandeling



7. Rechten van betrokkenen

7.1 Transparante communicatie

Voor G4S is het belangrijk dat medewerkers, klanten, leveranciers en andere stakeholders erop kunnen vertrouwen dat zijn of haar persoonsgegevens veilig en zorgvuldig worden verwerkt. Dat vertrouwen wordt gecreëerd door inzichtelijk te maken op welke wijze gegevens worden verwerkt en beheerd. Hierbij wordt duidelijk:

- Welke gegevens worden verzameld;
- Wat het doel is om deze gegevens te verzamelen;
- Wat er vervolgens met deze gegevens gebeurt;
- Wie toegang heeft tot de gegevens;
- Welke rechten betrokkenen hebben.

De informatie wordt op een zodanige wijze verstrekt dat de betrokkene de inhoud ervan begrijpt.

7.2 Recht van inzage van persoonsgegevens

Conform de GDPR heeft iedere betrokkene het recht om op te vragen welke persoonsgegevens van hem of haar voor welke doeleinden worden verwerkt. Een verzoek tot inzage van minderjarigen die de leeftijd van 16 jaar nog niet hebben bereikt, geschiedt door hun wettelijke vertegenwoordiger.

7.3 Recht op rectificatie van persoonsgegevens

Conform de GDPR heeft de betrokkene het recht om onverwijld zijn of haar persoonsgegevens te laten verbeteren, te wijzigen of aan te vullen, als deze feitelijk onjuist, onvolledig of niet ter zake zijn.

7.4 Recht op gegevenswissing

Conform de GDPR heeft betrokkene het recht zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen indien een van de volgende gevallen van toepassing is:

- De persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt;
- De betrokkene trekt de toestemming waarop de verwerking overeenkomstig artikel 6, lid 1, punt a) GDPR, of artikel 9, lid 2, punt a) GDPR, berust, in, en er is geen andere rechtsgrond voor de verwerking;
- De betrokkene maakt overeenkomstig artikel 21, lid 1 GDPR, bezwaar tegen de verwerking, en er zijn geen prevalerende dwingende gerechtvaardigde gronden voor

de verwerking, of de betrokkene maakt bezwaar tegen de verwerking overeenkomstig artikel 21, lid 2 GDPR;

- De persoonsgegevens zijn onrechtmatig verwerkt;
- De persoonsgegevens moeten worden gewist om te voldoen aan een in het Unierecht of het lidstatelijke recht neergelegde wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
- De persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij als bedoeld in de GDPR.

7.5 Recht op beperking van de verwerking

Conform de GDPR heeft iedere betrokkene het recht om bij G4S de beperking van de verwerking te verkrijgen indien een van de volgende elementen van toepassing is:

- De juistheid van de persoonsgegevens wordt betwist door de betrokkene, gedurende een periode die de verwerkingsverantwoordelijke in staat stelt de juistheid van de persoonsgegevens te controleren;
- De verwerking is onrechtmatig en de betrokkene verzet zich tegen het wissen van de persoonsgegevens en verzoekt in de plaats daarvan om beperking van het gebruik ervan;
- De verwerkingsverantwoordelijke heeft de persoonsgegevens niet meer nodig voor de verwerkingsdoeleinden, maar de betrokkene heeft deze nodig voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
- De betrokkene heeft overeenkomstig artikel 21, lid 1 GDPR bezwaar gemaakt tegen de verwerking, in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van de verwerkingsverantwoordelijke zwaarder wegen dan die van de betrokkene.

7.6 Recht op overdraagbaarheid van gegevens

Conform de GDPR heeft de betrokkene het recht de hem betreffende persoonsgegevens, die hij aan een verwerkingsverantwoordelijke heeft verstrekt, in een gestructureerde, gangbare en leesbare vorm te verkrijgen, en hij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden gehinderd door de verwerkingsverantwoordelijke aan wie de persoonsgegevens waren verstrekt, indien:

- De verwerking berust op toestemming uit hoofde van artikel 6, lid 1, punt a) GDPR, of artikel 9, lid 2, punt a) GDPR, of op een overeenkomst uit hoofde van artikel 6, lid 1, punt b) GDPR; en de verwerking via geautomatiseerde procedés wordt verricht.

7.7 Indienen verzoek

Verzoek tot inzage, rectificatie, gegevenswissing, beperking of overdraagbaarheid kan schriftelijk worden gestuurd naar Koning Boudewijnlaan 30, 1800 Vilvoorde, België, t.a.v. Data Protection Officer of per e-mail naar privacy.gdpr@be.g4s.com.

G4S reageert schriftelijk uiterlijk binnen vier weken op het verzoek. G4S draagt hierbij zorg voor een deugdelijke vaststelling van de identiteit van degene die het verzoek indient. Zodra het verzoek gerechtvaardigd is, neemt G4S onverwijld maatregelen die nodig zijn om aan het verzoek te voldoen.

Bij een besluit over een verzoek kan de betrokkene schriftelijk bezwaar indienen als hij of zij van mening is dat de wettelijke bepalingen betreffende de bescherming van persoonsgegevens niet correct zijn gehandhaafd. Indien de betrokkene niet akkoord gaat met het antwoord van G4S hierop, dan heeft de betrokkene de mogelijkheid verdere gerechtelijke stappen te ondernemen.

8. Tot slot

Dit beleid is vastgesteld door de directie van G4S België op 15 mei 2018. Eveneens werd de Ondernemingsraad omtrent dit beleidsdocument geïnformeerd.

Aanpassingen van dit beleid worden aangekondigd via de G4S website en de meest recente versie is gepubliceerd op www.g4s.be/privacy.

Voor vragen en/of opmerkingen met betrekking tot dit beleid kunt u terecht bij de privacy officer.