Privacy risicoscanrapport

in opdracht van

Divato IT Solutions

Uitgevoerd door	: mr. G. Erkaslan LLM, CIPP/e
Uitvoerend bureau	: Privacy Direct
Plaats, datum	: Haps, oktober 2019

Inleiding
In opdracht van Divato IT Solutions (hierna: Divato of de Verwerkingsverantwoordelijke) heeft Privacy Direct een Privacy Risicoscan (PRS) uitgevoerd om een goed beeld te krijgen van de maatregelen die door Divato zijn genomen ter bescherming van de privacy van zijn gebruikers. Daarmee ook ter implementatie van de regels uit de Algemene Verordening Gegevensbescherming (AVG) en aanverwante regels. De uitgevoerde Privacy Risicoscan heeft een goed beeld van hoe de privacyregels binnen Divato is gewaarborgd.

1. Algemene Vragen

Doeleinden gegevensverwerkingen
Divato verwerkt de persoonsgegevens voor welbepaalde doeleinden, namelijk voor het uitvoeren van de overeenkomsten met haar klanten en leveranciers, het bieden van ondersteuning aan de eindgebruikers van de geleverde IT-faciliteiten en ter naleving van de wet- en regelgeving die relevant zijn voor Divato. Divato maakt zelf ook gebruik van de diensten van derde-partijen, zoals Cloud computing dienstverlener in Nederland. Ook in dit kader is gegevensverwerking niet onbelangrijk.

Persoonsgegevens en derden
Divato verwerkt de persoonsgegevens in een interne omgeving voor het beheren van de administratie. Deze persoonsgegevens kunnen enkel worden ingezien door de bevoegde medewerkers binnen Divato. Externe partijen hebben geen direct toegang tot deze interne systemen en de daarin opgeslagen persoonsgegevens van de betrokkenen.

Divato deelt de persoonsgegevens waar nodig en mogelijk wel met externe partijen met wie zij samenwerkt. Deze partijen moeten dan een zakelijke relatie met Divato te hebben, anders worden de gegevens niet met deze partijen gedeeld. Hierbij kan men denken aan bijvoorbeeld de boekhouder/accountant, websitebouwer, Cloud hostingbedrijf.

Categorieën van persoonsgegevens
Divato verwerkt persoonsgegevens over de volgende categorieën van personen:

- (Oud-)medewerkers,
- Klanten
- Eindgebruikers van de website of IT-diensten zoals VoIP, Cloud of IT.

Divato verwerkt geen persoonsgegevens van specifieke groepen/categorieën persoonsgegevens, bijvoorbeeld bijzondere gegevens van zorgbehoevenden, mensen met een laag inkomen etc.

2. Organisatierisico's

Organisatierisico's kunnen zich voordoen, indien de intern betrokkenen kritische vragen stellen over de gegevensverwerkingen, en deze vragen nadelige gevolgen kunnen hebben voor de gegevensverwerkingen voor specifieke processen.

Divato heeft de afgelopen twee jaar geen kritische vragen over de privacyaspecten ten aanzien van de gegevensverwerkingen ontvangen van interne stakeholders. Vanuit de externe betrokkenen, voornamelijk (potentiële) klanten in de semipublieke sector waar veel bijzondere persoonsgegevens worden verwerkt en onderling worden uitgewisseld. Zij hebben voornamelijk vragen over de technische en organisatorische maatregelen die Divato heeft genomen ter bescherming van de persoonsgegevens van de betrokkenen. Divato heeft diverse maatregelen getroffen, deze maatregelen zullen in de volgende paragrafen worden behandeld.

Divato geeft aan de naleving van de privacyregels erg belangrijk te vinden en het erg zou vinden als de gegevensverwerkingen nadelige gevolgen zouden kunnen hebben voor business continuïteit, de stakeholders, de organisatiereputatie, kwaliteit van dienstverlening of zou leiden tot boetes wegens overtredingen.

Hiermee laat Divato niet alleen zien niet alleen commerciële doelen na te streven, maar tegelijkertijd ook zich bewust te zijn van het belang van naleving van wet- en regelgeving op het gebied van de privacy. Zo is Divato zich ervan bewust welke persoonsgegevens er worden verwerkt, wat deze gegevensverwerkingen voor de betrokkenen kunnen betekenen en welke gevoeligheden Divato hierbij kan verwachten.

3. Privacy risico's

De gegevensverwerkingen kunnen privacy risico's met zich meebrengen, welke risico's nadelige gevolgen voor de gehele organisatie en de bij de organisatie betrokken personen kunnen hebben. Het is van groot belang dat de organisatie goed in beeld heeft wat deze privacy risico's zijn, op welke wijze deze risico's zoveel mogelijk kunnen worden uitgesloten.

Divato verwerkt de persoonsgegevens op een systematische wijze, wat betekent dat Divato de persoonsgegevens regelmatig verwerkt, en deze gegevensverwerkingen niet sporadisch plaatsvinden of op onregelmatige wijze zijn.

De door Divato verwerkte persoonsgegevens zijn daadwerkelijk nodig om het doel te bereiken waarvoor deze persoonsgegevens worden verwerkt. Divato kan voor het bereiken van de gestelde doelen niet volstaan met statistische, gepseudonimiseerde of geaggregeerde persoonsgegevens. Divato maakt echter wel gebruik van technieken om de aanwezige persoonsgegevens in de aanwezige systemen waar nodig te anonimiseren, voor zover en indien dit noodzakelijk is. Dit kan zowel vanuit de klant c.q. leverancier worden gevraagd, als wel voortvloeien uit de toepasselijke wet- en regelgeving en aanbevelingen vanuit de brancheorganisatie.

Divato verwerkt c.q. bewaart persoonsgegevens voor welbepaalde doeleinden en weet wat er met deze persoonsgegevens wordt gedaan. De persoonsgegevens van ex-werknemers worden bewaard. Divato houdt bij het verwerken en opslaan van de persoonsgegevens rekening met de wettelijke bewaartermijnen. Deze bewaartermijnen worden ook intern gemonitord om termijnoverschrijdingen te voorkomen.

Divato verwerkt geen bijzondere categorieën van persoonsgegevens, zoals gegevens over de gezondheid, financiële positie of biometrische gegevens van de betrokkenen. Divato verwerkt persoonsgegevens met een verhoogde gevoeligheid, deze gegevens zijn gekoppeld aan eigen personeel van Divato, welke gegevens worden verwerkt voor een optimale bedrijfsvoering voor personeel, klanten en leveranciers.
Het is van belang dat Divato de juiste persoonsgegevens kan verwerken voor het bereiken van de doelen waarvoor deze persoonsgegevens worden verzameld. Persoonsgegevens met een verhoogde gevoeligheid mogen wettelijk niet worden verwerkt zonder een duidelijk doel. Divato verwerkt deze specifieke persoonsgegevens voor de betaling van de salarissen van haar medewerkers, wat een wettelijke grondslag is voor het verwerken van deze persoonsgegevens door Divato. De verwerkte persoonsgegevens zijn niet toegankelijk voor een grote groep van mensen, de kring van gegevensverwerkers is door Divato beperkt tot enkel de daartoe bevoegde interne medewerkers.

Divato verwerkt geen persoonsgegevens om persoonlijke aspecten van een natuurlijk persoon te evalueren en daarmee het gedrag of handelingen te analyseren dan wel te

voorspellen, dit wordt profiling genoemd. Wel kunnen de online omgevingen c.q. platforms die Divato aanbiedt, door de klant worden ingezet voor geautomatiseerde besluitvorming. Divato heeft geen mogelijkheid om deze wijze van gegevensverwerkingen door de klant te beïnvloeden.

Divato verwerkt de persoonsgegevens verder voor direct marketing doeleinden of dienstverlening op basis van de locatie van betrokkenen (bijvoorbeeld via een website met gepersonaliseerde advertenties) of het tracken van het gebruik van websites of online diensten, zoals cookies. Het gaat om de persoonsgegevens van zowel natuurlijke als zakelijke personen om inzicht te krijgen waar de behoeften van de klanten van Divato liggen. Het is van belang dat Divato voor dit doel persoonsgegevens gebruikt die daarvoor nodig zijn, niet te veel of juist te weinig persoonsgegevens. In de zin van de Algemene Verordening Gegevensbescherming wordt dit ook dataminimalisatie genoemd. Divato voldoet hiermee ook aan het beginsel van dataminimalisatie.

Verder worden de aanwezige persoonsgegevens gedeeld met externe partijen die in opdracht van Divato diensten uitvoeren en daarbij persoonsgegevens van klanten, werknemers en eventueel andere betrokkenen nodig hebben. De persoonsgegevens die in beheer van Divato zijn, worden niet gekoppeld aan klantenbestanden van externe partijen. Evenmin worden deze persoonsgegevens voor commerciële doeleinden verstrekt aan derde-partijen met wie Divato samenwerkt.

Divato heeft een privacyverklaring waarin de doelen, de omvang van de gegevensverwerkingen en de rechten van betrokkenen zijn vermeld. De betrokkenen worden waar nodig ook geïnformeerd over hun rechten onder de AVG. Daarnaast houdt Divato uitdrukkelijk rekening met de geldende bewaartermijnen voor het opslaan van de aanwezige persoonsgegevens van betrokkenen. Deze bewaartermijnen worden bovendien gemonitord om te voorkomen dat deze persoonsgegevens onnodig lang worden bewaard.

Divato verwerkt de persoonsgegevens binnen de Europese Economische Ruimte (Europese Unie aangevuld met Noorwegen, IJsland en Liechtenstein). Hiermee wordt voldaan aan de eis van de AVG dat persoonsgegevens niet buiten de Europese Economische Ruimte worden verwerkt. De persoonsgegevens worden niet getransporteerd naar landen buiten de Europese Economische Ruimte zoals hierboven omschreven. De serverlocatie van de opgeslagen persoonsgegevens worden zowel fysiek als technisch beveiligd. Zo is er geen toegang tot deze locatie voor onbevoegden. De locatie is beveiligd met zichtbare en niet zichtbare maatregelen om de servers te beveiligen. Daarnaast heeft Divato duidelijke afspraken gemaakt met haar ketenpartners om de bescherming van de persoonsgegevens van de betrokkenen te waarborgen. In de meeste gevallen zijn de afspraken neergelegd in een verwerkersovereenkomst tussen Divato en de tegenpartij.

4. Privacy management

Privacy management is een belangrijk onderdeel van de implementatie van de privacyregels binnen iedere organisatie, zo ook binnen Divato. In beginsel maakt het niet uit wat de kerntaken van een organisatie zijn. Echter, hoe meer persoonsgegevens er binnen een organisatie verwerkt, dan wel hoe meer bijzondere persoonsgegevens er worden verwerkt, des te belangrijker het wordt dat de organisatie maatregelen treft. De aard en de omvang van de getroffen maatregelen kunnen per organisatie dan ook verschillen. Een goed werkend privacy management is dan onmisbaar voor iedere organisatie.

Privacy management houdt in dat de organisatie blijft waken over actuele privacyregels en een accuraat beleid op het gebied van privacy- en informatiebeveiliging. In de voorgaande paragrafen hebben wij kunnen zien dat Divato uit de AVG voortvloeiende privacyregels erg belangrijk vindt, en daaromtrent de nodige maatregelen heeft getroffen.

Zo is duidelijk te zien wie er binnen Divato de eindverantwoordelijke is voor het proces of systeem waarbinnen de gegevensverwerkingen plaatsvinden. De verantwoordelijke hiervoor is namelijk de directie van Divato. Het is voor de eindverantwoordelijke duidelijk welke taken en bevoegdheden verbonden zijn aan privacy- en gegevensbescherming.

Divato beschikt over een register van alle verwerkingsactiviteiten (verwerkingsregister). Hierin is onder meer opgenomen welke persoonsgegevens er worden verwerkt, voor welke doeleinden en hoelang. Ook is er duidelijk vermeld met welke partijen deze persoonsgegevens worden uitgewisseld en welke afspraken onderling zijn gemaakt ter bescherming van de betreffende persoonsgegevens van de betrokkenen.

Ook beschikt Divato over een geschreven privacybeleid. Hierin is opgenomen op welke wijze er binnen Divato invulling wordt gegeven aan de wet- en regelgeving op het gebied van bescherming van persoonsgegevens en privacy van de betrokkenen.

De door Divato genomen technische en organisatorische maatregelen worden periodiek geëvalueerd. Indien Divato deze maatregelen consequent naleeft, kan blijvend voldoen aan de strenge privacyregels die voortvloeien uit de AVG. Hiermee wordt door Divato ook invulling gegeven aan de naleving van de compliance-regels. Dit biedt de klanten een grotere mate van zekerheid over de naleving van de regels door Divato.

5. Privacy volwassenheidsniveau

De mate van naleving van de privacyregels door een organisatie wordt ook gemeten door het privacy volwassenheidsniveau. Dit zegt in het kort over de vraag hoe organisaties omgaan met de persoonsgegevens en welke maatregelen zij nemen om de privacy van de betrokkenen blijvend te waarborgen.

Het privacy volwassenheidsmodel kent vijf volwassenheidsniveaus, 1 t/m 5. Het volwassenheidsniveau 0, waarbij een organisatie zich niet druk maakt om privacy, behandelen wij hier niet. Wanneer privacy binnen een organisatie situationeel is ingericht, komt deze organisatie niet hoger dan niveau 1.

Op niveau 2 is grip op privacy gebaseerd op beslissingen die door meerdere personen gezamenlijk op een vastgelegde wijze worden genomen. Op dit niveau is er dan sprake van beheerste processen, maar is de aantoonbaarheid van hoe aan de wet- en regelgeving wordt voldaan beperkt.

Op niveau 3 werkt de organisatie organisatiebreed aan privacy en kan dit worden aangetoond. Niveau 3 kan aldus als een minimumniveau worden gezien om aan de wet- en regelgeving te voldoen. Simpelweg omdat de wet- en regelgeving de aantoonbaarheid vereist.

Door de volwassenheid van de organisatie op niveau 4 te brengen wordt niet alleen aan de wet- en regelgeving voldaan, maar kan er ook actief op wijzigingen worden geanticipeerd. Op niveau 5 is privacy een speerpunt op alle niveaus binnen de organisatie geworden en krijgt het ook aandacht in communicatie-uitingen naar publiek of klanten.

Hieronder worden de volwassenheidsniveaus nader uitgewerkt, waarna in de volgende paragraaf wordt aangegeven wat het privacy volwassenheidsniveau binnen Divato is.

5.1 Privacy volwassenheidsniveaus nader toegelicht

Hierna worden de privacy volwassenheidsniveaus nader toegelicht en uitgewerkt.

5.1.1 Niveau 1 – Informeel

Op niveau 1 verzamelt en verwerkt een organisatie persoonsgegevens, waarbij de keuzes per gegevensverwerking op verwerkingsniveau worden gemaakt vanuit persoonlijk perspectief en afhankelijk zijn van de kennis en kunde van individuele medewerkers. Hierbij ontbreekt het aan formele processen om eisen te stellen aan de verwerking van persoonsgegevens en worden er informeel keuzes gemaakt over hoe er in een concreet geval wordt omgegaan met persoonsgegevens en op welke wijze de gegevens worden verzameld en (verder) verwerkt. Dit betekent dat op dit niveau wel vastlegging kan plaatsvinden, maar dat er geen sprake is van vaststelling.

Daarnaast is er geen managementcyclus, waardoor reactief wordt gereageerd op keuzes en incidenten die zich voordoen.

5.1.2 Niveau 2 – Beheerst proces

De organisatie verwerkt en verzamelt persoonsgegevens, waarbij keuzes worden gemaakt op basis van operationeel beleid, richtlijnen en werkinstructies dat door de verwerkingsverantwoordelijke wordt gedeeld en niet meer per gegevensverwerking wordt bepaald.

Op dit niveau zijn het beleid, de richtlijnen en werkinstructies per afdeling vastgelegd, maar sluiten niet noodzakelijkerwijs aan op de organisatiebrede omgang met persoonsgegevens.

5.1.3 Niveau 3 – Vastgesteld proces

Op dit niveau verwerkt de organisatie persoonsgegevens, waarbij keuzes zijn gemaakt op basis van beleid, richtlijnen en instructies op organisatieniveau. De naleving van beleid, richtlijnen en instructies wordt actief aangestuurd door de directie. De bestuurder is betrokken bij de handhaving van het beleid en de uitvoering, waarbij gerapporteerd wordt ondersteund door controlemiddelen en informatie. Dit leidt tot een lerend proces binnen de hele organisatie.

5.1.4 Niveau 4 – Voorspelbaar proces

Op dit niveau verzamelt en verwerkt de organisatie persoonsgegevens, waarbij wordt gestuurd op snelheid en kwaliteit van de interacties. Het beleid en de uitvoering ervan wordt continu bewaakt en waar nodig bijgewerkt om de organisatiebrede beleidsdoelen te behalen. Het lerend vermogen in de uitvoerende en specifiek beleidsmatige laag is voorspelbaar.

5.1.5 Niveau 5 – Geoptimaliseerd

Op dit niveau is er een sterk en expliciet verband tussen externe eisen, beveiligingsdoelstellingen, algemeen beleid, specifiek beleid en uitvoering van het beleid. Aan alle keuzes (van de directie red.) ligt een uitgebreide, nauwkeurige analyse ten grondslag. Hierdoor kan de organisatie snel reageren op de veranderingen in wet- en regelgeving op het gebied van informatiebeveiliging en gegevensbescherming. Bovendien is de organisatie in staat om voorafgaand prognoses af te geven over kosten en baten bij naleving van wet- en regelgeving. Daardoor kan de organisatie weloverwogen keuzes maken en de uitkomsten van de beleidskeuzes voorspellen en aansturen.

5.2 Privacy volwassenheidsniveau Divato

Op basis van de beschikbare informatie, de beleidsdocumenten en de tussen Divato en haar partners gemaakte afspraken, concluderen wij dat het privacy volwassenheidsniveau 3 van toepassing is. Divato verwerkt de persoonsgegevens, waarbij keuzes zijn gemaakt op basis van beleid, richtlijnen en instructies op organisatieniveau. De naleving van beleid, richtlijnen

en instructies wordt actief aangestuurd door de directie. De directie is direct betrokken bij de handhaving van het beleid en de uitvoering. Binnen de hele organisatie is sprake van een lerend proces.

Op basis van deze bevindingen kunnen wij concluderen dat Divato de nodige technische en organisatorische maatregelen heeft getroffen om een adequaat niveau van bescherming van de persoonsgegevens en informatiebeveiliging te realiseren. Divato is in staat om de privacy van haar klanten en eindgebruikers te beschermen en de uit de Algemene Verordening Gegevensbescherming voortvloeiende regels conform het privacy volwassenheidsniveau 3 na te leven.