AVG protocol It's Public - versie 10 mei 2022

Belang van goed omgaan met persoonsgegevens

It's Public vind het belangrijk dat persoonsgegevens goed worden beschermd. De beveiliging van persoonsgegevens hangt af van technische en organisatorische maatregelen die zijn genomen. Technische maatregelen (zoals veilige elektronische systemen en overzichtelijke mapstructuren) zorgen ervoor dat persoonsgegevens niet vrij toegankelijk zijn voor onbevoegden. Organisatorische maatregelen, zoals verwerkingsregisters en - protocollen, zorgen ervoor dat de persoonsgegevens ook daadwerkelijk veilig en overzichtelijk worden verwerkt.

Adviesopdrachten

Een belangrijk onderdeel van ons AVG beleid is het omgaan met persoonsgegevens die wij ontvangen van opdrachtgevers voor het uitvoeren van projecten. Hieronder wordt beschreven welke acties wij bij elke opdracht nemen in het kader van het AVG beleid.

Vóór opdracht

Er is sprake van verwerking persoonsgegevens in het kader van de AVG als er (een combinatie aan) gegevens worden gebruikt die, indien de data openbaar gepubliceerd zou worden, door enig persoon met andere (openbare) bronnen gecombineerd zou kunnen worden tot identificatie van de persoon (bijv. combi postcode en geboortedatum), is er sprake van verwerking van persoonsgegevens in kader AVG.

Vooraf wordt bepaald of dit nodig is in het kader van het project. Als er een manier is om dit te voorkomen dan heeft dat de voorkeur (bijv. niet geboortedatum gebruiken, maar geboortemaand, waardoor het minder snel herleidbaar is).

Als er met persoonsgegevens gewerkt moet worden, vul dan in het projectvoorstel de bijlage 'Persoonsgegevens te verwerken in kader van deze opdracht' in en vraag expliciet toestemming aan de opdrachtgever (deze bijlage mag anders verwijderd worden).

Start opdracht

1. Bij aanvang (na consent verwerkingsovereenkomst) van het project wordt bepaald wie de AVG-verantwoordelijke is in het project.
2. De AVG verantwoordelijke documenteert alle aangeleverde data in het 'Projecten' tabblad in het AVG verwerkingsregister. Eventuele afwijkende termijnen en/of acties worden erin verwerkt.

Tijdens opdracht

Handel altijd in lijn met de veiligheidsvoorschriften zoals benoemd in de bijlage bij de Algemene Voorwaarden. Bevestig dat alle teamleden dit hebben doorgenomen en voldoen.

Een paar belangrijke aandachtspunten:

- Bestanden waarin persoonsgegevens voorkomen, worden in een aparte map opgeslagen waar niet alle It's Public medewerkers bij kunnen.
- Als je emails ontvangt met bijlagen waarin vertrouwelijke persoonsgegevens voorkomen, geef deze dan een label. Zo kun je deze na afloop van de opdracht makkelijk terugvinden en verwijderen.
- Mochten er tijdens de opdracht nieuwe/aanvullende data (persoonsgegevens) gebruikt worden die eerder niet voorzien waren, dan wordt er opnieuw toestemming gevraagd aan de opdrachtgever en wordt het verwerkingsregister aangevuld.

Einde opdracht

1. Na het afronden van de opdracht wordt door de AVG verantwoordelijke consultant in het 'Projecten verwerkingsregister' ingevuld dat de opdracht is opgeleverd. De bewaartermijn van ontvangen data gaat nu in.
2. Na verstrijken bewaartermijn (6 maanden of aparte afspraak):
    a. Alle bestanden en e-mails met vertrouwelijke persoonsgegevens worden verwijderd of geanonimiseerd
    b. Indien vastgesteld bij start opdracht worden overige acties ondernomen

Algemene bedrijfsvoering

It's Public verzamelt en verwerkt verschillende persoonsgegevens als onderdeel van algemene bedrijfsvoering, bijv. bij websitegebruik, nieuwsbriefaanmeldingen, kennismakingsevenementen, sollicitaties en interne bedrijfsvoering (werknemers) verschillende soorten persoonsgegevens. In het AVG Verwerkingsregister houden we overzicht op de verwerking en beveiliging van deze gegevens.

Als wij in het kader van onze bedrijfsvoering persoonsgegevens verwerken, dan zullen wij altijd bepalen of het verzamelen van persoonsgegevens strikt noodzakelijk is.

Verzoek tot het inzien, aanpassen of verwijderen van gegevens

Personen die gebruik maken van onze diensten en waarvan persoonsgegevens worden verzameld hebben verschillende rechten ten aanzien van deze gegevens. Zo hebben o.a. lezers van onze nieuwsbrief, (potentiële) sollicitanten en personen van wie wij gegevens hebben ontvangen in ons projectwerk het recht om hun persoonsgegevens in te zien, te corrigeren of te verwijderen. Daarnaast hebben zij het recht om eventuele toestemming voor de gegevensverwerking in te trekken of bezwaar te maken tegen de verwerking van hun persoonsgegevens door It's Public. Bovendien kunnen zij een verzoek indienen om de betreffende, door ons verwerkte persoonsgegevens naar hen toe te sturen.

Wanneer wij een van de mail met een van de voorgenoemde verzoeken ontvangen, moeten de volgende stappen worden doorlopen.

Stap 1: xx zal als privacy officer verantwoordelijk zijn voor de juist en tijdige uitvoer van de vraag. Mocht een andere medewerker een verzoek of vraag met betrekking tot verwerking van persoonsgegevens ontvangen, dan dient deze direct de privacy officer op de hoogte te stellen.

Stap 2: De privacy officer zal acties ondernemen om aan het verzoek van de betreffende persoon (of personen) te voldoen nadat duidelijk is:

1) Duidelijk is wat het verzoek precies inhoudt
2) Duidelijk is wie het verzoek doet en degene(n) zich met een bijgevoegde identiteitsdocument heeft geïdentificeerd (hierbij moet BSN, MRZ en eventueel paspoortnummer worden zwart gelakt t.b.v. privacy)

Stap 3: De privacy officer reageert zo snel mogelijk, maar uiterlijk binnen 4 weken, op het verzoek.

Datalek

Ondanks alle beveiligingsmaatregelen valt het echter nooit volledig te voorkomen dat er een datalek zal plaatsvinden. It's Public is op grond van de Algemene verordening gegevensbescherming (AVG) verplicht om (ernstige) datalekken te melden aan de Autoriteit Persoonsgegevens en aan betrokkenen. Dit document formuleert de stappen die genomen moeten worden mocht er onverhoopt een datalek plaatsvinden.

1 Definitie datalek

Er is sprake van een datalek als er een inbreuk op de beveiliging plaatsvindt die per ongeluk of op onrechtmatige wijze leidt tot vernietiging, wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens. Van een datalek is dus al sprake wanneer je (per ongeluk) een verkeerd document (bijvoorbeeld van een ander project) verstuurd aan een opdrachtgever en dit document persoonsgegevens bevat. Een datalek gaat dus niet enkel om het hacken van websites en e-mailadressen.

2. Interne verantwoordelijke melding datalekken

It's Public heeft een AVG-verantwoordelijke voor de verwerking van datalekken aangesteld die verantwoordelijk is voor de melding van een datalek. Deze verantwoordelijke is xxx, hierna te noemen: 'Privacy officer'.

3. Interne melding bij ontdekking van een datalek

1. Degene die een datalek bij It's Public ontdekt, meldt dit zo spoedig mogelijk aan de intern verantwoordelijke.
2. Indien mogelijk zorgt degene die het datalek heeft ontdekt er gelijktijdig voor dat de gelekte gegevens meteen op afstand worden gewist of ontoegankelijk gemaakt.

4. Onderzoek door interne verantwoordelijke

De interne verantwoordelijke onderzoekt onder meer:

1. Of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden.
2. Wie of welk projectteam binnen de organisatie betrokken zijn bij het datalek.
3. Of er een verwerker betrokken is bij het incident.

5. Bestrijding datalek

De interne verantwoordelijke stopt het datalek indien dat nog kan en neemt de noodzakelijke maatregelen om het datalek zo goed mogelijk te bestrijden.

6. Vaststelling van de gevolgen van een datalek

De interne verantwoordelijke onderzoekt de mogelijke gevolgen van het datalek aan de hand van de aard en de omvang van de gegevens die gelekt zijn en stelt vast wat de nadelige gevolgen van betrokkenen kunnen zijn.

7. Medewerking verstrekking gegevens omtrent het datalek

De ontdekker/melder van het datalek biedt alle medewerking aan de interne verantwoordelijk door zo snel en zo goed mogelijk (schriftelijk) antwoord te geven op de volgende vragen:

1. Wat is er gebeurd? (omschrijving van het incident)
2. Ging het per ongeluk of is het veroorzaakt door kwade opzet (denk aan gehackte gegevens)?
3. Wanneer is het gebeurd? (datum en tijdstip)
4. Wanneer is het ontdekt?
5. Wat voor gegevens (registers) zijn gelekt?
6. Zijn de gegevens versleuteld, en zo ja: hoe?
7. Konden de gegevens op afstand worden gewist of ontoegankelijk gemaakt, en zo ja, is dat gebeurd?
8. Wat zijn de mogelijke gevolgen voor de betrokkenen?
9. Welke groep(en) personen is /zijn hierdoor getroffen? (bijvoorbeeld: leerlingen, patiënten, premium leden)
10. Hoeveel personen zijn hierdoor (bij benadering) getroffen?
11. Zijn er ook gegevens van personen in andere EU-landen getroffen door het datalek?
12. Konden er al technische en/of organisatorische maatregelen worden getroffen naar aanleiding van het incident?

8. Beschikbaarheid personeel na ontdekking datalek

De verantwoordelijke van de afdeling vanuit waar het datalek heeft plaatsgevonden alsook de ontdekker van het datalek en iedereen die vanuit hun functie of kennis in staat is om organisatorische en/of technische maatregelen te treffen om de gevolgen van het datalek te beperken, houden zich de 1e 24 uur na ontdekking van het datalek beschikbaar voor overleg met de interne verantwoordelijke (of eventueel door hem aangewezen experts) en voor het zo nodig uitvoeren van opgedragen werkzaamheden als gevolg van het datalek.

9. Beslissing melding datalekken

1. De interne verantwoordelijke beslist zo spoedig mogelijk doch in elk geval binnen 48 uur na ontdekking van het datalek – al dat niet in overleg met de verantwoordelijke van de afdeling vanuit waar het datalek is ontdekt en/of door hem aangewezen experts – of het datalek dient te worden gemeld aan de Autoriteit Persoonsgegevens en/of de betrokkenen.
2. Een datalek wordt in principe altijd gemeld aan de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van de betrokkenen.
3. De melding van het datalek gaat gepaard met beantwoording van de vragen zoals omschreven in onderdeel 7.

4. Een datalek dat gemeld is aan de Autoriteit Persoonsgegevens wordt ook gemeld aan de betrokkenen als het lek een risico vormt voor hun rechten en vrijheden, tenzij inmiddels passende maatregelen zijn genomen die het hoge risico hebben afgewend.

10. Melding datalekken aan de Autoriteit Persoonsgegevens en/of betrokkenen

1. De interne verantwoordelijke draagt zo nodig zorg voor de melding aan de Autoriteit Persoonsgegevens en/of de betrokkene(n).
2. De interne verantwoordelijke doet zo spoedig mogelijk melding en uiterlijk binnen 72 uur na ontdekking van het datalek.
3. Het is andere werknemers (buiten de interne verantwoordelijke) niet toegestaan om het (mogelijke) datalek zelf aan de Autoriteit Persoonsgegevens en/of de betrokkene(n) te melden.
4. Als een werknemer het niet eens is met de beslissing van de interne verantwoordelijke over het al dan niet melden van het datalek aan de Autoriteit Persoonsgegevens en/of de betrokkene(n), dan kan hij dit kenbaar maken aan de directie.
5. Mocht het worden verzocht, dan verlenen werknemers alle medewerking aan de verantwoordelijke om de getroffen personen conform artikel 34 AVG te kunnen informeren over het datalek.

11. Gevolgen melding datalekken

1. In het geval dat het datalek negatieve gevolgen heeft voor betrokkenen, dan doet de interne verantwoordelijke er alles aan om deze gevolgen zoveel mogelijk te beperken.
2. Afhankelijk van de aard en omvang van het datalek voor betrokkenen bepaalt de interne verantwoordelijke:
    - op welke wijze betrokkenen worden geïnformeerd (waaronder in ieder geval de mededelingen worden gedaan welke soorten persoonsgegevens getroffen zijn, wat de mogelijke gevolgen zijn, welke maatregelen It's Public neemt en op welke wijze betrokkenen zelf de schade kunnen voorkomen of beperken)
    - welke nazorg betrokkenen krijgen
    - welke acties in het belang van de organisatie noodzakelijk zijn
3. Indien een datalek heeft plaatsgevonden – ongeacht of deze is gemeld of niet – worden zo spoedig mogelijk adequate technische en/of organisatorische maatregelen getroffen om toekomstige gelijksoortige datalekken te voorkomen.

12. Bijhouden register datalekken

De interne verantwoordelijke houdt een register bij van alle datalekken, waarin alle gegevens rondom het datalek worden geregistreerd, zoals:

1. Een omschrijving van het incident

2. Datum en tijdstip van het datalek
3. Datum en tijdstip ontdekking van het datalek
4. Omschrijving van de soort gelekte persoonsgegevens omschrijving van de categorie(en van betrokkenen die zijn getroffen
5. Omschrijving aantal betrokkenen (bij benadering)
6. Of ook gegevens van personen in andere EU-landen zijn gelekt
7. Of het incident is gemeld aan de Autoriteit Persoonsgegevens en zo ja datum en tijdstip melding
8. Of het incident is gemeld aan de betrokkenen en zo ja, datum en tijdstip
9. Welke technische en/of organisatorische maatregelen zijn getroffen na het datalek, met vermelding van datum en tijdstip