Memo

Bestuursdienst

aan:

van:

kopie aan:

datum: 6 juni 2018

bestand: M:\Mijn documenten\Informatiebeveiligingsbeleid\Documenten in Informatiebeveiligings- en privacybeleid\Beleid verstrekken persoonsgegevens aan medewerkers.v05.docx

onderwerp: Beleid m.b.t. het verstrekken van persoonsgegevens aan OU medewerkers

Om te kunnen voldoen aan de AVG heeft de Open Universiteit o.a. beleid nodig voor het verstrekken van persoonsgegevens aan OU medewerkers. Het betreft persoonsgegevens waarvoor de OU de verantwoordelijke is en waarbij de betrokkenen[1] onze studenten en/of medewerkers zijn (interne medewerkers en extern door de OU ingehuurde medewerkers). Persoonsgegevens van personen die hun gegevens alleen aan de OU hebben verstrekt om informatie van de OU te vragen (belangstellenden), worden nooit verstrekt.

Afhankelijk van het doel waarvoor de persoonsgegevens zullen worden gebruikt, onderscheiden we drie situaties waarin persoonsgegevens aan medewerkers kunnen worden verstrekt.

Situaties

A. Onderzoek
   Waar persoonsgegevens worden gevraagd voor wetenschappelijk onderzoek, dient de aanvrager het door de commissie Ethische Toetsing Onderzoek (cETO) goedgekeurde onderzoeksplan te overleggen. In zo'n plan wordt beschreven van welke groepen betrokkenen de gegevens worden verwerkt en welke attributen per betrokkene worden verwerkt. Op grond van een door de cETO goedgekeurd onderzoeksplan kunnen de daarin genoemde persoonsgegevens worden verstrekt.

B. Bedrijfsvoering
   Waar persoonsgegevens worden gevraagd voor toepassing in de bedrijfsvoering van de OU, dient de aanvrager een daartoe ontworpen Aanvraagformulier in te vullen en te overleggen.
   Dit betreft in het algemeen processen (en daarmee aanvragen) die regelmatig worden herhaald. Voor nieuwe aanvragen en voor aanvragen waar – vergeleken met eerdere aanvragen – additionele persoonsgegevens worden opgevraagd, is toestemming van de dataeigenaar en de Privacy Officer (PO) vereist. Bij escalatie zal de verwerking bij de Functionaris voor de gegevensverwerking (FG) worden getoetst.

C. Andere
   Bij andere situaties vindt de aanvraag ook plaats middels het eerder genoemde Aanvraagformulier. Daarbij is altijd toestemming van de dataeigenaar en de PO vereist. Bij escalatie zal de verwerking bij de FG worden getoetst.

[1] *Betrokkenen* zijn de personen waarop de persoonsgegevens betrekking hebben.

Registratie van de verstrekking

De persoonsgegevens worden aan de aanvragers verstrekt door de *medewerker managementinformatie* binnen KenC, verder te noemen: de *verstrekker*. Bij elke verstrekking van persoonsgegevens o.g.v. dit beleid, zal de verstrekker de inhoud van het Aanvraagformulier controleren en bij ongerijmdheden overleggen met de PO. De verstrekker archiveert de Aanvraagformulieren en zal die op verzoek aan de FG ter beschikking stellen. De verstrekkingen zullen o.g.v. de gearchiveerde ingevulde Aanvraagformulieren worden vastgelegd in het betreffende dataregister, welk wordt beheerd door de FG.

Aanvraagformulier

Met het eerder genoemde digitale Aanvraagformulier worden minimaal de volgende gegevens uitgevraagd:

- de identiteit, het organisatieonderdeel en de functie/rol van de aanvrager,
- een (verwijzing naar) de beschrijving van het betreffende bedrijfsproces of de andere situatie waarin de persoonsgegevens zullen worden gebruikt,
- het doel van verwerking waarvoor de aangevraagde persoonsgegevens zullen worden gebruikt,
- de doelbinding,
- een lijst of omschrijving van de gewenste betrokkenen,
- de attributen die per betrokkene worden verwerkt,
- de uiterste datum waarop de ontvanger de ontvangen persoonsgegevens zal vernietigen.

Maatregelen voor het waarborgen van de privacy

De aanvrager is vanaf het moment van de verstrekking verantwoordelijk voor het voldoen aan de privacy wet- en regelgeving m.b.t. de verstrekte persoonsgegevens. Dat betreft met name het beschermen van die gegevens tegen onrechtmatige verwerking zoals verwerking door onbevoegden of verwerking voor een doel waarvoor de betrokkene geen toestemming heeft gegeven.

Als dat verenigbaar is met het onderzoek of de toepassing, verdient het aanbeveling de verstrekte persoonsgegevens te anonimiseren of te pseudonimiseren (vraag zo nodig advies). Na anonimiseren is er geen sprake meer van persoonsgegevens en hoeven er geen maatregelen meer te worden getroffen om de privacy te waarborgen. Wellicht is de vertrouwelijkheid nog wél van belang! Denk er aan om na het anonimiseren of pseudonimiseren de oorspronkelijke persoonsgegevens adequaat te vernietigen (zie beneden).

1. Bewaren
   Bewaar de verstrekte persoonsgegevens op een veilige plaats, bij voorkeur op de centrale ict-voorzieningen van de OU in een map waarop de toegangsrechten zodanig zijn ingesteld dat de toegang is voorbehouden aan de OU medewerkers die uit hoofde van hun functie toegang nodig hebben.

   Als de verstrekte persoonsgegevens noodzakelijkerwijs buiten de centrale ict-voorzieningen van de OU moeten worden bewaard of verwerkt – bijvoorbeeld op een niet OU desktop computer, op een mobiele client of op een externe gegevensdrager – zorg dan dat de toegang tot het betreffende apparaat is beveiligd. Bewaar het apparaat daartoe in een afgesloten kast of ruimte en zorg dat de toegang tot het apparaat is beveiligd met een wachtwoord of pincode. Een veilige lengte van een wachtwoord of een pincode wordt mede bepaald door de gevoeligheid van de persoonsgegevens. Gevoelige persoonsgegevens mogen – buiten de centrale ict-voorzieningen van de OU – alleen in versleutelde vorm worden bewaard.

   Persoonsgegevens mogen alleen *in de cloud* worden bewaard of verwerkt indien de OU een bewerkersovereenkomst heeft afgesloten met de aanbieder van de betreffende clouddienst. Let er ook op dat persoonsgegevens op een mobiele client niet op een onveilige plaats (bijvoorbeeld in de cloud) worden geback-upt.

2. Versturen
   Persoonsgegevens mogen buiten de OU alleen op beveiligde wijze worden verstuurd (verplaatst). Gebruik bij het versturen over internet altijd HTTP**S** of VPN. E-mail is niet veilig. Indien persoonsgegevens via e-mail worden verstuurd, moeten de persoonsgegevens versleuteld zijn. Daarbij mag de sleutel niet per e-mail worden verstuurd maar moet via een ander kanaal, bijvoorbeeld telefonisch, worden doorgegeven.

3. Vernietigen
   Ook na het einde van het onderzoek of de toepassing mogen de persoonsgegevens niet op een onveilige plaats achterblijven. Bij mobiele clients of externe gegevensdragers is het niet voldoende om de gegevens te deleten. Vraag advies over een adequate methode van vernietiging.

   Respecteer de bewaartermijn van de verstrekte gegevens. Bij Onderzoek ligt die termijn vast in het onderzoeksplan. Bij de andere toepassingen is de vernietigingsdatum vermeld op het aanvraagformulier.

4. Delen
   De verstrekte persoonsgegevens mogen niet worden gedeeld met personen die niet in dienst zijn van de OU, behalve na schriftelijke toestemming van de dataeigenaar en de PO. Bij escalatie zal het verzoek bij de FG worden getoetst.

5. Publiceren
   Bij het einde van het onderzoek of de toepassing zijn er vaak resultaten die openbaar gemaakt moeten worden. Bij onderzoek zal de cETO zich daarover hebben uitgesproken. Ook bij andere toepassingen moet worden geborgd dat de privacy van de betrokkenen door de publicatie niet wordt geschaad. Het is vaak mogelijk om alleen geaggregeerde gegevens te publiceren. In andere gevallen zullen de betrokkenen in de publicatie alsnog geanonimiseerd moeten worden.

Advies

Vraag bij twijfel advies aan de Privacy officer (privacyofficer@ou.nl).