Universiteit Utrecht

Privacy-checklist

Deze checklist helpt je zorgvuldig en volgens de wetgeving te werken met de persoonsgegevens van o.a. medewerkers en studenten[1].

Wil je gebruiken maken of maak je reeds gebruik van persoonsgegevens van medewerkers, studenten en/of gasten van de UU? Doorloop dan de volgende stappen:

1. Loop de privacy-checklist door om te controleren of er nog bepaalde stappen vereist zijn om te zorgen dat het gebruik van de persoonsgegevens voldoet aan alle wettelijke eisen;
2. Vul het bijgevoegde Registratieformulier privacygevoelige gegevensverzameling (bijlage II);
3. Stuur het vervolgens aan de privacy-contactpersoon van je afdeling of faculteit;
4. De privacy-contactpersoon zal eventuele knelpunten met je bespreken en je helpen om een oplossing hiervoor te vinden;
5. De directeur van je faculteit of dienst moet de gegevensverzameling goedkeuren;
6. De privacy-contactpersoon zal het goedgekeurde formulier ter registratie toesturen aan de Functionaris Gegevensbescherming (FG) van de UU. Je weet dan zeker dat je volgens de privacyrichtlijnen van de UU hebt gehandeld.

Waarom deze checklist?
De privacy van zowel studenten als medewerkers is voor de Universiteit Utrecht (UU) van groot belang. Op het verwerken van persoonsgegevens is de Wet bescherming persoonsgegevens (Wbp) van toepassing die vereist dat er zorgvuldig met persoonsgegevens wordt omgegaan, zodat de privacy van de betrokkenen wordt gewaarborgd. Vanaf 25 mei 2018 wordt de Wbp vervangen door de Europese Algemene verordening gegevensbescherming. Deze checklist houdt daar al rekening mee.

Meer informatie
Raadpleeg de handleiding bij de checklist voor een nadere toelichting bij de verschillende vragen.

Heb je vragen of twijfel je over het (voorgenomen) gebruik van persoonsgegevens? Neem dan contact op met de Functionaris Gegevensbescherming via privacy@uu.nl.

[1] Dit document heeft geen betrekking op het registreren van persoonsgegevens voor onderzoeksdoeleinden (bijvoorbeeld sociale of medische gegevens). Informatie over de (wettelijke) regels voor het veilig omgaan met persoonsgegevens voor onderzoeksdoeleinden is te verkrijgen bij de onderzoeksleider van je afdeling.

Universiteit Utrecht

Privacy-checklist[2]

Een korte toelichting bij onderstaande vragen is opgenomen in de handleiding Privacy-checklist (bijlage II). Als je na het lezen ervan nog vragen over de checklist of over het omgaan met persoonsgegevens hebt, kun je contact opnemen met de Functionaris Gegevensbescherming van de UU (privacy@uu.nl).

1. **Welke directeur is verantwoordelijk voor het verwerken van de gegevens?**
2. **Zijn er bijzondere persoonsgegevens verzameld en zo ja, welke?**
3. **Wat is het doel waarvoor de persoonsgegevens zijn verzameld?**
4. **Zijn deze gegevens noodzakelijk om dit doel te bereiken?**
5. **Zijn de gegevens oorspronkelijk ook voor dit doel verzameld?[3]**
6. **Worden de gegevens uitsluitend opgeslagen binnen door de UU goedgekeurde systemen?**
7. **Zijn de gegevens passend beveiligd, gelet op de mate van gevoeligheid van de gegevens?**
8. **Zijn de personen van wie gegevens worden verwerkt, erover geïnformeerd?**
9. **Zijn er bewaartermijnen vastgesteld en worden deze gecontroleerd en nageleefd?**
10. **Is de verwerking van de persoonsgegevens gedocumenteerd?**

[2] Het formulier is bedoeld voor de registratie van bestaande maar ook voor die van nieuwe verzamelingen van persoonsgegevens.

[3] Persoonsgegevens die voor administratieve doeleinden zijn vastgelegd, mogen worden gebruikt voor historisch, wetenschappelijk of statisch onderzoek. Hier zitten echter wel een aantal restricties aan. Zo mogen de persoonsgegevens niet ingezet worden om op individueel niveau beslissingen te nemen over een persoon. De uitkomsten van onderzoek mogen dus niet worden gebruikt om bijvoorbeeld een bepaalde student te weigeren voor een studie. Ook mag de rapportage over het onderzoek nooit gebeuren op individueel niveau en mogen de resultaten nooit te herleiden zijn tot individuele personen.

Universiteit Utrecht

Bijlage I

Handleiding privacy-checklist

Deze handleiding geeft een toelichting op de bovenstaande privacy-checklist.

1. Verantwoordelijkheid voor het verwerken van gegevens

Ten eerste dient er bij alle gegevens die verwerkt gaan worden, ongeacht of dat persoonsgegevens zijn of niet, vastgesteld te worden welke directeur verantwoordelijk is voor het verwerken van deze gegevens. Welke afdeling trekt bijvoorbeeld de kar bij een bepaald project, of wie heeft de zeggenschap over bepaalde gegevens? Voordat gegevens worden verwerkt, dient de verantwoordelijke directeur toegewezen te worden.

De directeur onder wiens verantwoordelijkheid bepaalde gegevens worden verzameld, is verantwoordelijk voor de bescherming van de privacy van de personen om wie het gaat, en voor de bescherming van de gegevens op zich (zie punt 7 van de privacy-checklist).

2. (Bijzondere) persoonsgegevens

Ieder gegeven over een direct of indirect te herleiden (al dan niet anoniem) individu is een persoonsgegeven. In ons geval kunnen persoonsgegevens gaan over bijvoorbeeld studenten, medewerkers of Uithofbezoekers. Denk hierbij aan naam- en adresgegevens, maar ook aan een studentnummer, e-mailadres, CV, verzuim- of verlofgegevens en camerabeelden. Ook een IP-adres en sommige cookies zijn persoonsgegevens.

Persoonsgegevens zijn per definitie privacygevoelig. Toch worden sommige gegevens a priori als gevoelig ingeschat. Dit worden ook wel bijzondere persoonsgegevens genoemd Deze gegevens mogen alleen verwerkt worden indien dat is vastgelegd in de wet en er passende beveiligingsmaatregelen zijn genomen, zie hiervoor punt 7. Voorbeelden van gevoelige gegevens zijn studieresultaten, BSN, gegevens over iemands ras, politieke en seksuele voorkeuren en medische en strafrechtelijke gegevens.

Houd er rekening mee dat pasfoto's, nationaliteit of de voornaam van iemand zijn of haar partner ook aangemerkt kunnen worden als bijzondere persoonsgegevens omdat zij indirect iets kunnen vertellen over de persoon in kwestie, bijvoorbeeld de seksuele voorkeur, afkomst of etniciteit.

3. Doel van het gebruik van de persoonsgegevens

Zijn of worden de gegevens gebruikt voor een eenduidig, en wettelijk toegestaan doel? En is dit doel ook vastgelegd in een plan van aanpak of in het beleid? Neem bij twijfel contact op met de Functionaris Gegevensbescherming om te controleren of het ook wettelijk is toegestaan om de gegevens voor dit doel te verwerken.

Het doel van het verzamelen van bepaalde persoonsgegevens zal je van tevoren vaststellen, dus voordat je de gegevens gaat verzamelen. Op basis daarvan kan de wettelijke grondslag worden bepaald waarop de gegevensverwerking kan worden gebaseerd.

Het doel van de gegevensverzameling moet je documenteren (zie punt 10 van de privacy-checklist) en laten goedkeuren door de Functionaris Gegevensbescherming. De afweging van het organisatiebelang bij de gegevensverwerking tegenover de privacybelangen van de betrokkenen is daarbij wezenlijk, net als de noodzakelijkheid van het verzamelen van de specifiek gewenste gegevens (zie punt 4 van de privacy-checklist).

4. Noodzaak van de gegevensverzameling

Enkel gegevens die, gelet op het doel van de verzameling, onmisbaar zijn mogen worden gebruikt volgens de Wbp. Gegevens die slechts wenselijk of handig zijn, mogen dus niet worden gebruikt. Voor statistisch onderzoek zijn namen, geboortedata of volledige adressen vaak niet nodig. Beperk het gebruik in die situaties bijvoorbeeld tot geboortejaren en de vier cijfers van de postcode om correlaties te maken.

Je moet van tevoren zeker weten dat je alleen met deze gegevens het doel van het verzamelen kunt bereiken en dat het doel niet op een andere, minder privacygevoelige manier te bereiken is. Tevens dient daarbij rekening gehouden te worden met het privacybelang van het individu. Het doel van de gegevensverzameling moet worden vastgelegd en goedgekeurd door de Functionaris Gegevensbescherming (zie punt 3 van de privacy-checklist).

5. Oorspronkelijk doel van de gegevensverzameling

Het is mogelijk dat gegevens die in de eerste instantie voor een specifiek doel zijn verzameld, vervolgens voor een ander doel worden gebruikt. Voorbeeld: je maakt een bestand aan met e-mailadressen van studenten zodat je een bevestiging kunt versturen van de inschrijving. Je mag de e-mailadressen dan dus niet gebruiken om studenten per e-mail uit te nodigen voor een seminar.

Als je een reeds bestaande gegevensverzameling wilt hergebruiken, moet je vaststellen of het doel overeenkomt met het doel waarvoor de gegevens oorspronkelijk verzameld zijn. Als dat niet zo is, kun je deze privacy-checklist gebruiken om vast te stellen of je de gegevens wel voor het nieuwe doel mag gebruiken: zijn bijvoorbeeld de gegevens noodzakelijk om het doel te bereiken, zijn de betreffende personen van het nieuwe gebruik op de hoogte, etc. Geef in ieder geval aan wat het bronsysteem van de gegevens is (Osiris, SAP, etc.).

6. Door de UU goedgekeurde systemen

Om de veiligheid van de persoonsgegevens te waarborgen is het zaak dat ze uitsluitend opgeslagen worden in systemen van de UU, of in systemen van door de UU goedgekeurde leveranciers. Het is niet toegestaan om persoonsgegevens buiten deze systemen om op te slaan, dus ook niet op je eigen laptop of USB-stick. De UU kan de veiligheid van de andere systemen immers niet garanderen. Informeer bij de Functionaris Gegevensbescherming of een systeem is goedgekeurd door de UU.

UU-goedgekeurde systemen zijn systemen van de UU zelf of systemen van leveranciers waarmee de UU een overeenkomst over het gebruik ervan heeft afgesloten. De UU moet ervoor kunnen instaan dat de genomen veiligheidsmaatregelen voldoende zijn en dat de verwerking van de gegevens gebeurt op een wijze die door de UU is goedgekeurd.

7. Gegevensbeveiliging

Gegevens moeten ‘passend’ beveiligd worden. Wat passend is hangt af van het soort gegevens dat verwerkt wordt. Hoe gevoeliger de gegevens, hoe beter de beveiliging moet zijn. Zo kunnen gegevens versleuteld worden, en kan toegang tot gegevens worden beperkt door een select aantal medewerkers toegang te verschaffen tot de gegevens. Uitgangspunt is in ieder geval dat alleen diegenen die de gegevens per se nodig hebben erbij mogen kunnen.

Afhankelijk van de classificatie van de gegevens zijn er verschillende beveiligingsniveaus gedefinieerd. Zo hebben algemene gegevens een lager beveiligingsniveau nodig dan persoonsgegevens. Bijzondere persoonsgegevens moeten op het hoogste niveau beveiligd worden. Ook de omvang van de gegevensverzameling bepaalt het niveau van de beveiliging. Een groter bestand heeft in principe een hoger beveiligingsniveau nodig dan een klein bestand. Daarnaast is het van belang dat alleen voor de medewerkers voor wie het noodzakelijk is bij de uitvoering van hun werkzaamheden, dienen toegang te hebben tot de gegevens.

Het is noodzakelijk dat je van tevoren vaststelt hoe privacygevoelig de verzamelde gegevens en wat (dus) noodzakelijke beveiligingsmaatregelen zijn, door een zogeheten 'gegevensclassificatie' uit te voeren. De Corporate Information Security Officer (CISO) van de UU of de Local Information Security Officer (LISM) van je faculteit kan je daarbij helpen.

8. Personen op de hoogte stellen van de verwerking

Transparantie is belangrijk bij de omgang met persoonsgegevens. De personen op wie de gegevens betrekking op hebben moeten weten waarvoor hun gegevens gebruikt worden. Personen van wie je gegevens verzamelt, moet je daarover dus tijdig inlichten en ze daarbij op de hoogte stellen van het doel van de gegevensverzameling.

Het informeren over het gebruik van persoonsgegevens kan gebeuren via een rechtstreeks bericht aan de betreffende personen of via een algemene mededeling op de website waar de gegevens worden verzameld. De personen moeten daarbij in de gelegenheid worden gesteld om aan te geven dat zij bezwaar hebben tegen de opname van hun gegevens in de gegevensverzameling.

9. Bewaartermijn van de gegevens

Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk is. Als de persoonsgegevens niet meer nodig zijn om het beoogde doel te verwezenlijken, dienen ze verwijderd te worden op het moment dat de afgesproken bewaartermijn is verstreken.

De wet heeft een aantal bewaartermijnen vastgesteld. Zo is er een bewaartermijn vanuit de Belastingdienst vastgesteld van zeven jaar voor financiële gegevens, gelden er diverse bewaartermijnen voor het bewaren van het personeelsdossier, zoals vijf jaar na uitdiensttreding van de medewerker. Indien er geen wettelijke bewaartermijn is vastgesteld, dan dient de bewaartermijn vastgesteld te worden door de Functionaris Gegevensbescherming. Informeer daarom bij de FG wat een redelijke bewaartermijn is voor de gegevens die jij wilt verwerken. De directeur is ervoor verantwoordelijk dat de afgesproken bewaartermijnen ook daadwerkelijk worden nageleefd.

Universiteit Utrecht

10. Documentatie van het gebruik van de persoonsgegevens

De verantwoordelijke directeur, genoemd bij vraag 1, dient het gebruik van de gegevens te documenteren. Dit kan door het 'Registratieformulier privacygevoelige gegevens' in te (laten) vullen (zie bijlage II).

De wijze van verzamelen, het gebruik van de persoonsgegevens en de daarmee verband houdende aspecten zoals beveiliging en verantwoordelijkheid moeten controleerbaar zijn en gehandhaafd kunnen worden.

De informatie over gegevensverzamelingen zal worden opgenomen in een centraal register van de UU, dat wordt beheerd door de Functionaris Gegevensbescherming.

Universiteit Utrecht

Bijlage II

Registratieformulier privacygevoelige gegevensverzamelingen

A.	*Verantwoordelijke directeur*	
B.	*Soort persoonsgegevens*	
C.	*Doel waarvoor de gegevens zijn verzameld*	
D.	*Wijze waarop de gegevens zijn verzameld*	
E.	*Systeem of bestand waarin de gegevens worden zijn opgeslagen en worden verwerkt*	
F.	*Wijze waarop de gegevens zijn beveiligd*	
G.	*Wijze waarop de betrokkenen zijn geïnformeerd*	
H.	*Bewaartermijn van de gegevens*	
I.	*Categorieën verwerkers die toegang tot de persoonsgegevens hebben*	
J.	*Contactgegevens van de (in- of externe) verwerker(s) van de gegevens*	