Bestuurszaken

ALGEMEEN PRIVACYBELEID

2023

VRIJE UNIVERSITEIT AMSTERDAM

STATUS Definitief
VERSIE: 1.0 – t.b.v. openbare publicatie

AUTEUR Bestuurlijke en Juridische Zaken
DATUM 20-06-2023

Inhoud

1. INLEIDING EN DOEL

In dit document wordt beschreven hoe de Vrije Universiteit Amsterdam (hierna: '**VU**') omgaat met haar wettelijke verplichtingen in het kader van de bescherming van persoonsgegevens (hierna: '**privacy**'). Het is bedoeld om inzichtelijk te maken hoe de VU privacy heeft georganiseerd en welke processen daarbij moeten worden gevolgd. In het beleid wordt zoveel mogelijk aansluiting gezocht bij bestaande organisatie- en werkprocessen van de VU.

Dit document is niet bedoeld om betrokkenen te informeren over gegevensverwerkingen van de VU. Dit wordt gedaan in de verschillende reglementen (zie hoofdstuk 4.2). Meer informatie is ook te vinden op de website van de VU: Privacy Statement Vrije Universiteit Amsterdam - More about - Vrije Universiteit Amsterdam (vu.nl)

2. TOEPASSELIJKHEID

Dit beleid is een gegevenbeschermingsbeleid in de zin van artikel 24 van de Algemene verordening gegevensbescherming (hierna: '**AVG**'). Het beleid is van toepassing op alle onderdelen van de VU.

3. MISSIE EN RISICOBEREIDHEID

Het privacybeleid sluit aan bij de missie en de kernwaarden van de VU om met wetenschappelijk en waardengedreven onderwijs, onderzoek en valorisatie, verantwoordelijkheid voor mens en planeet te nemen op een verantwoordelijke, open en transparante manier.

Onze privacymissie is dan ook om ervoor te zorgen dat de persoonsgegevens van studenten, onderzoeksdeelnemers, medewerkers en andere betrokkenen zorgvuldig, transparant en in overeenstemming met wet- en regelgeving verwerkt worden.

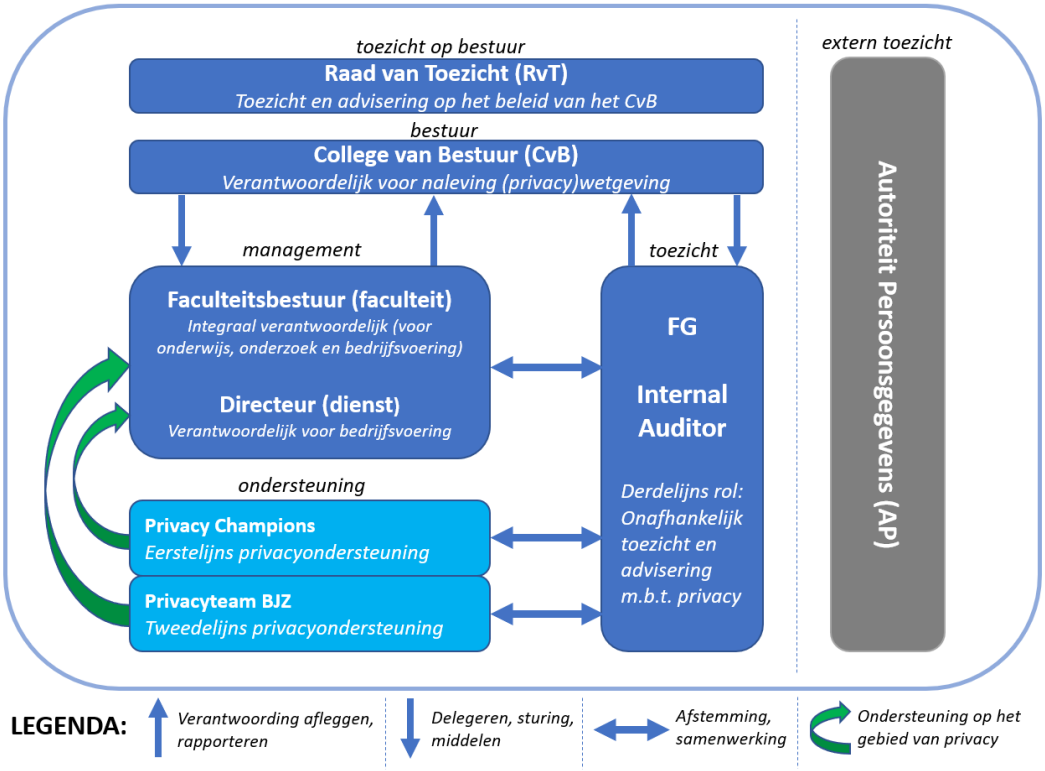
De risicobereidheid ten aanzien van privacy is laag. Dit is in overeenstemming met de risicobereidheid van de VU ten aanzien van andere compliance-vraagstukken. Een lage risicobereidheid betekent niet dat overtredingen van wet- en regelgeving zijn uitgesloten, maar betekent wel dat privacy een vast en goed geborgd onderdeel zijn in het onderwijs, het onderzoek en de bedrijfsvoering van de VU.

4. DE PRIVACYORGANISATIE

Dit hoofdstuk beschrijft hoe de VU haar privacyorganisatie heeft ingericht. Er wordt zoveel mogelijk aansluiting gezocht bij bestaande structuren en het besturingsmodel van de VU.

4.1. ORGANISATIE

De privacyorganisatie van de VU is ingericht conform het 'three lines model'[1]. De afbeelding hieronder geeft hiervan een samenvatting. **Bijlage 1** geeft een nadere invulling van de verschillende verantwoordelijkheden en taken. Beschikbare tijd, (persoonlijke) expertise en bovenal collegialiteit zijn factoren die mede bepalen wie wat op welk moment doet.



4.1.1. EERSTELIJN – LIJNVERANTWOORDELIJKHEID

Conform het besturingsmodel van de VU[2] geldt dat verantwoordelijkheden zo laag mogelijk in de organisatie worden neergelegd. Dat betekent dat elke faculteit en dienst verantwoordelijk is voor haar eigen compliance met wet- en regelgeving en het privacybeleid. Dit betekent ook dat medewerkers zelf verantwoordelijkheid dragen. Zo is een afdelingshoofd verantwoordelijk voor zijn afdeling, een teamleider voor zijn team en een onderzoeker verantwoordelijk voor zijn onderzoek.

Binnen het faculteitsbestuur is de directeur bedrijfsvoering de portefeuillehouder van privacy. Binnen een dienst is de directeur (eind)verantwoordelijk voor privacy.

[1] Three Lines Model Updated – juli 2020 – The Institute of Internal Auditors.
[2] Besturingsmodel VU – 30 juni 2015: Beschrijving van het besturingsmodel van de VU.

4.1.1.1. Leidinggevende

Elke leidinggevende heeft de taak om:

- ervoor te zorgen dat zijn/haar medewerkers op de hoogte zijn en blijven van de voor hen relevante aspecten van het privacybeleid en wetgeving; en
- toe te zien op de naleving van het privacybeleid binnen haar processen, systemen en/of afdeling.

4.1.1.2. Privacy Champions

Elke faculteit en dienst heeft minstens één Privacy Champion. De Privacy Champion is het eerste aanspreekpunt voor medewerkers met vragen op het gebied van privacy. De Privacy Champion heeft een eerstelijns ondersteunde rol en signalerende rol. Bij complexe privacyvraagstukken haakt de Privacy Champion het Privacyteam van BJZ aan voor tweedelijns ondersteuning. Het volledige profiel van een Privacy Champion staat in **Bijlage 2**.

Elke faculteit en dienst heeft één of meerdere Privacy Champion(s) aangesteld. Om een goed werkende en laagdrempelige eerste lijn te hebben worden eenheden aangemoedigd om meer capaciteit voor Privacy Champions vrij te maken.

Wanneer een eenheid een Privacy Champion aanstelt, meldt zij dat bij Bestuurlijke en Juridische Zaken.

4.1.2. TWEEDE LIJN – BESTUURLIJKE EN JURIDISCHE ZAKEN

De afdeling Bestuurlijke en Juridische Zaken (hierna: '**BJZ**') maakt hoogwaardige juridische expertise laagdrempelig, toegankelijk, hoe complex het vraagstuk ook is. BJZ is verantwoordelijk voor de juridische advisering rondom privacy, het in stand houden en verbeteren van het netwerk van Privacy Champions, het beschikbaar hebben van benodigde systemen en het verzorgen van trainingen op het terrein van privacy. Hiermee levert BJZ een actieve bijdrage aan de privacy compliance van de VU en helpt zij de eerste lijn invulling te geven aan hun verantwoordelijkheden.

BJZ stemt af met aanpalende disciplines (zoals informatiebeveiliging, research data management, documentmanagement en kennisveiligheid) om ervoor te zorgen dat het privacybeleid van de VU blijft aansluiten op de andere vakgebieden.

Zie ook bijlage 1 voor een uitsplitsing van de activiteiten van BJZ.

4.1.3. DERDE LIJN – FUNCTIONARIS VOOR DE GEGEVENSBESCHERMING

De AVG verplicht de VU om een functionaris gegevensbescherming (hierna: '**FG**') aan te stellen. De FG houdt toezicht op de toepassing en naleving van de privacywetgeving door de VU. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie.

De FG is aanspreekpunt en vraagbaak voor betrokkenen die vragen hebben over de bescherming van persoonsgegevens. Daarnaast coördineert de FG het datalekproces en geeft advies met betrekking tot de gegevensbeschermingseffectbeoordelingen (DPIA's). De FG is het eerste aanspreekpunt voor de Autoriteit Persoonsgegevens (AP).

Ten slotte vervult de internal auditor van de VU als onafhankelijke functionaris, naast de FG, VU-breed het derdelijns toezicht. De internal auditor ziet toe op de effectiviteit van de privacy governance, het risicomanagement en de interne beheersmaatregelen. De internal auditor geeft gevraagd en ongevraagd advies aan het management, het CvB en/of de RvT.

Zie ook bijlage 1 voor een uitsplitsing van de activiteiten van de derde lijn.

4.1.4. EINDVERANTWOORDELIJK – COLLEGE VAN BESTUUR

Het College van Bestuur (CvB) is eindverantwoordelijk voor compliance met wet- en regelgeving. Het CvB stelt het beleid, de maatregelen en de procedures rondom verwerkingen van persoonsgegevens vast met dit privacybeleid.

4.2. Privacyreglementen, werkprocessen en PCF

Naast dit beleid heeft de VU verschillende documenten waarin het onderwerp privacy is geregeld. Er zijn drie typen documenten te onderscheiden:

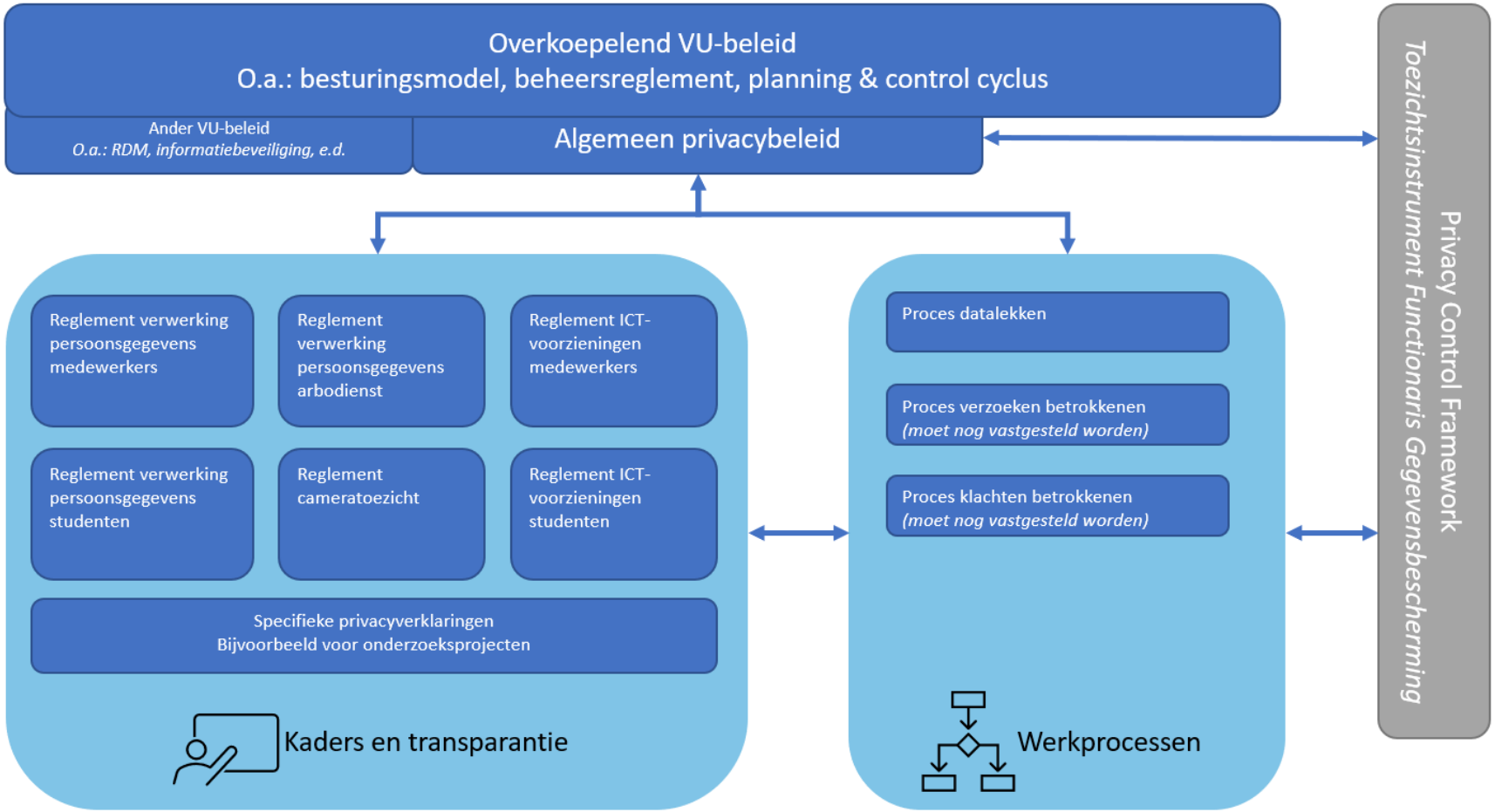
1. Privacyreglementen en privacyverklaringen
   Deze bieden VU-brede kaders en dienen als een middel om transparant te zijn over wat voor verwerkingen van persoonsgegevens de VU doet. Voor specifieke verwerkingen stelt de VU specifieke privacyverklaringen op. Een voorbeeld hiervan is de privacyverklaring over de website op VU.nl.

   Met betrekking tot wetenschappelijk onderzoek en valorisatie heeft de VU geen algemeen reglement. Dit omdat de verwerkingen in die domeinen zo divers zijn dat betrokkenen geïnformeerd worden via specifieke privacyverklaringen.

2. Werkprocessen
   Bepaalde processen met betrekking tot privacy zijn vastgelegd in documenten. Dit zijn bijvoorbeeld:
   a. Proces datalekken;
   b. Proces verzoeken betrokkenen; en
   c. Proces privacyklachten.

3. Privacy Control Framework (PCF)
   Het PCF is een risicobeheersings-systeem voor privacy compliance binnen de VU, waarmee inzichtelijk kan worden gemaakt hoe de VU de interne beheersing voor privacy compliance aantoonbaar heeft vormgegeven. Het PCF van de VU maakt onderdeel uit van het Business Control Framework van de VU. Het PCF wordt beheerd en bijgehouden door de FG.

4.2.1. VISUELE WEERGAVE PRIVACYBELEID



5. RAPPORTEREN EN VERBETEREN

Om de hiervoor genoemde doelen en verantwoordelijkheden te laten werken, is privacy opgenomen in de planning & control cyclus van de VU. Concreet betekent dit dat faculteiten en diensten in hun jaarplan het onderwerp privacy meenemen en rapporteren over de voortgang. Het College van Bestuur houdt hierdoor inzicht en overzicht en heeft een basis om de Raad van Toezicht geïnformeerd te houden.

In de **Bijlage 3** staat de opzet voor de rapportage. Deze opzet is zoveel mogelijk gebaseerd op de huidige structuur van de planning & control cyclus.

6. BIJLAGE 1 – ROLVERDELING (RACI)

NIET OPENBARE BIJLAGE

7. BIJLAGE 2 – PROFIEL PRIVACY CHAMPION

Inleiding
Privacy en gegevensbescherming zijn belangrijke onderwerpen voor de VU. Vanaf mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. De AVG brengt nieuwe vraagstukken en verplichtingen met zich mee. Om deze het hoofd te kunnen bieden, is kennis en gezamenlijke inspanning nodig. Faculteiten en diensten zijn er verantwoordelijk voor dat hun gegevensverwerkingen voldoen aan de wettelijke eisen. Het privacyteam van BJZ biedt hierbij ondersteuning, maar dit kan niet zonder de hulp van zogenoemde “Privacy Champions” die als eerste aanspreekpunt op een faculteit of dienst fungeren voor alle vragen op het gebied van privacy.

Wie zijn Privacy Champions?
De Privacy Champion is het eerste aanspreekpunt op de faculteit of binnen de dienst voor medewerkers die vragen hebben op het gebied van privacy. De Privacy Champion levert een actieve en enthousiaste bijdrage aan de bewustwording rondom het onderwerp privacy binnen een (onderdeel van een) faculteit of dienst. De Privacy Champion hoeft niet *alles* te weten van privacy. Hij/zij hoeft geen jurist of informatiebeveiliger te zijn, maar moet wel affiniteit met het onderwerp hebben en bereid zijn zich te blijven ontwikkelen op dit vlak.

De Privacy Champion is zichtbaar en toegankelijk. Hij/zij brengt het onderwerp privacy (proactief) onder de aandacht van zijn collega’s en biedt eerstelijnsondersteuning. De Privacy Champion beantwoordt de meest voorkomende privacyvragen, zoals: Mogen wij deze persoonsgegevens verwerken zonder toestemming van de betrokkenen? Heeft de VU een verwerkersovereenkomst met de leverancier van deze applicatie? Mag de VU persoonsgegevens doorgeven aan deze organisatie?

De Privacy Champion herkent ingewikkelde privacyvraagstukken en weet de weg te vinden naar het Privacyteam van BJZ. Ook helpt de Privacy Champion bij het signaleren van datalekken en de afhandeling hiervan. Daarnaast biedt de Privacy Champion ondersteuning bij het uitvoeren Data Protection Impact Assessments (DPIA’s).

Ten slotte zijn de Privacy Champions de ogen en oren van het privacyteam van BJZ. De Privacy Champions weten wat er op hun afdeling speelt en waar in de praktijk behoefte aan is. Zij hebben korte lijnen naar het privacyteam van BJZ.

Om ervoor te zorgen dat Privacy Champions beschikken over de juiste kennis en op de hoogte zijn en blijven van de laatste ontwikkelingen worden zij getraind door het privacyteam van BJZ volgens het principe ‘train de trainer’. Optionele aanvullende externe scholing dient door de eenheden zelf gefinancierd te worden.

In de **bijlage** is het profiel van de Privacy Champion gevoegd.

Profiel 'Privacy Champion'

Werkzaamheden

De Privacy Champion levert een actieve en enthousiaste bijdrage aan de bewustwording rondom het onderwerp privacy binnen de faculteit of dienst. De Privacy Champion is het eerste aanspreekpunt voor de faculteit of dienst op het gebied van privacy. Daarnaast biedt de Privacy Champion ondersteuning bij het invullen van het Register van verwerkingsactiviteiten van de VU en het uitvoeren Data Protection Impact Assessments (DPIA's). Verder is Privacy Champion de eerste contactpersoon binnen een faculteit of dienst voor het privacy-team van BJZ. De werkzaamheden van de contactpersoon zullen het volgende omvatten:

- het leveren van een bijdrage aan de bewustwording rondom privacy binnen de faculteit of dienst;
- het beantwoorden van eenvoudige vragen binnen de faculteit of dienst op het gebied van privacy (eerstelijnsondersteuning);
- het bieden van ondersteuning bij het uitvoeren van Data Protection Impact Assessments (DPIA'S);
- het doorzetten van complexere vraagstukken naar het privacy-team en/of andere diensten en waar nodig het vervullen van een coördinerende rol daarin;
- het signaleren van risico's op het gebied van privacy binnen de faculteit of dienst en waar nodig het terugkoppelen hiervan aan het privacy-team van BJZ;
- het signaleren van (mogelijke) datalekken en het bieden van ondersteuning bij de afhandeling hiervan; en
- het leveren van een bijdrage aan de verbetering van de informatievoorziening met betrekking tot privacy binnen de faculteit of dienst.

Opleiding, kennis en ervaring

- HBO/academisch werk- en denkniveau;
- kennis en ervaring op het gebied van de (bedrijfs)processen binnen de faculteit of dienst;
- kennis en ervaring op het gebied van (onderzoeks)projecten en het vervullen van een coördinerende rol;
- kennis van bescherming van persoonsgegevens (privacy) of de bereidheid deze op te doen; en
- kennis van informatiebeveiliging of de bereidheid deze op te doen.

Competenties

- goede communicatieve vaardigheden, zowel mondeling als schriftelijk;
- goed kunnen samenwerken met verschillende disciplines op verschillende niveaus; • alert, initiatiefrijk en omgevingsbewust; en
- bereid zijn zich te blijven ontwikkelen op dit vlak.

8. BIJLAGE 3 – OPZET RAPPORTAGE P&C-CYCLUS

Om op te nemen in de P&C-cyclus. Rapportage vindt plaats tijdens de P4, P8 en P12.

8.1. PRIVACY

In dit hoofdstuk geeft de eenheid aan hoe zij ervoor staat qua naleving van het privacybeleid en hoe zij haar privacy-compliance het komend jaar gaat verbeteren. Neem bij eventuele vragen over dit hoofdstuk contact op met Bestuurlijke en Juridische Zaken (BJZ). Indien u twijfelt over de meest effectieve acties voor het volgende jaar kunt u altijd contact opnemen met BJZ en/of de Functionaris Gegevensbescherming.

Houdt u er rekening mee dat er op het gebied van informatiebeveiliging rapportageverplichtingen gelden vanuit het strategische informatiebeveiligingsbeleid.

	Prioriteiten / doelstellingen behaald of op schema
	Prioriteiten / doelstellingen deels wel, deels niet behaald of op schema
	Prioriteiten / doelstellingen niet behaald of niet op schema

8.1.1. VU-BREDE PRIVACY PRIORITEITEN

Geef in onderstaande tabellen aan welke acties uw eenheid gaat uitvoeren. Geef een korte toelichting waarom voor deze acties is gekozen en welk doel is gesteld, oftewel bij welk resultaat de eenheid tevreden is.

Prioriteiten VU-breed			
Onderwerp	**Beschrijf wat de situatie in uw eenheid op dit moment is**	**Beschrijf welk doel is gesteld en welke acties u gaat uitvoeren in het komende jaar om daar te komen**	**Voortgang prioriteiten** (deze kolom pas invullen bij de 12-maandsrapportage, kolom wel laten staan in het jaarplan. Indien mogelijk graag kwantificeren)
Accuraatheid en volledigheid verwerkingsregister *(PrivacyPerfect en DMPonline)*			 *+ toelichting*
Privacybewustzijn			
Bezetting privacy champions			
Inzicht in en grip op samenwerkingen en leveranciers. Hoe is uw overzicht m.b.t. het delen van persoonsgegevens met externe partijen. Bijvoorbeeld in onderzoeksconsortia.			

8.1.2. CONCRETE VERBETERPLANNEN

Geef in deze paragraaf antwoord op de volgende vragen:

- *Wat is voor het volgend jaar uw top 3 van prioriteiten (naast die in de vorige paragraaf), welke uitdagingen heeft u daarbij en wat heeft u daarvoor nodig?*
- *Kunnen er ook activiteiten beëindigd worden? Welke zijn dat en waarom worden deze beëindigd?*

	Prioriteiten 202X		
A. Concrete verbeteracties	**B. Prioriteiten en doelstellingen voor 2023**	**C. Prioriteiten gereed per:**	**D. Voortgang prioriteiten** *(deze kolom pas invullen bij de 12-maandsrapportage, kolom wel laten staan in het jaarplan)*
Prioriteit 1: …			 *+ toelichting*
Prioriteit 2: …			
Prioriteit 3: …			