Privacy code en privacy regels
Nyenrode Business Universiteit

versie 1.4

31 juli 2017

Inhoudsopgave

Totstandkoming

Dit document is opgesteld door het Academic Services Center, naar aanleiding van het besluit van het CvB om het hoofd ASC als verantwoordelijke voor de bescherming persoonsgegevens aan te wijzen. Bij het opstellen is (met toestemming) dankbaar gebruik gemaakt van het privacy document van Universiteit Twente en van het Nyenrode policy document, zoals vastgesteld door het CvB op 31 juli 2017.

1 Privacy verklaring NBU

Nyenrode Business Universiteit (NBU) respecteert de persoonlijke levenssfeer van studenten, deelnemers, alumni, medewerkers en anderen. Met het onderhavige privacy beleid maakt NBU inzichtelijk hoe privacy bescherming is geregeld.

Tot 25 mei 2018 verwerkt NBU persoonsgegevens conform de Wet bescherming persoonsgegevens (Wbp), daarna geldt de Algemene verordening gegevensbescherming (Avg).

NBU verwerkt en verstrekt persoonsgegevens aan derden uitsluitend op basis van een wettelijke grondslag. Naast grondslag en doelbinding worden ook andere kernthema's uit de Avg in dit document uitgewerkt: transparantie, dataminimalisatie en beveiliging. Informatie wordt niet langer bewaard dan nodig voor het doel waarvoor deze is verzameld (dataminimalisatie). Informatie wordt niet gebruikt voor doelen die hier niet mee verenigbaar zijn (doelbinding).

Voor de administratie van onderwijs en bedrijfsvoering worden persoonsgegevens verzameld, zoals naam, e-mailadres, telefoonnummer, woonadres, gegevens over (voor)opleiding, studievoortgang, facturatie en gegevens die betrekking hebben op overige onderwijs gerelateerde studenten- en personeelsaangelegenheden. De gegevens worden in de meeste gevallen door de betrokkenen zelf verstrekt, maar kunnen ook afkomstig zijn uit bronsystemen van derden, bijvoorbeeld de IND en het ABP.

Via de website worden gegevens verzameld, voornamelijk ten behoeve van de studentenwerving, zoals bijvoorbeeld aanmeldingen voor open dagen of het opvragen van informatie.

Voor wetenschappelijk onderzoek worden gegevens verzameld in overeenstemming met de VSNU richtlijnen voor wetenschappelijk onderzoek, waar nodig na toetsing door de Nyenrode Commissie voor Wetenschappelijke Integriteit, en, indien relevant, wordt er melding gemaakt bij de functionaris voor de gegevensbescherming (FG).

Bij de verwerking van persoonsgegevens in bedrijfsvoering, onderzoek en administratie van onderwijs gaat NBU uit van het proportionaliteitsprincipe: de verwerking van persoonsgegevens moet proportioneel zijn aan het beoogde bedrijfsvoering- of onderzoeksdoel. Er wordt telkens een afweging gemaakt om het juiste evenwicht te vinden tussen privacy, bedrijfsvoering en onderzoeksdoelstelling.

Persoonsgegevens worden adequaat beveiligd en zo zorgvuldig als mogelijk behandeld. Er is aandacht voor informatiebeveiliging en privacy binnen NBU alle processen en activiteiten.

2 Privacy beleid

In onze toenemend gedigitaliseerde maatschappij krijgt privacy steeds meer aandacht. Medewerkers, studenten, deelnemers en anderen vinden privacy en bescherming van persoonsgegevens steeds belangrijker, mede door risico's voor organisaties en mogelijke aantasting van de persoonlijke levenssfeer. De Wbp is onlangs uitgebreid met een meldplicht datalekken, en op Europees niveau is recent de Algemene verordening gegevensbescherming (Avg) vastgesteld, als opvolger van de huidige richtlijn waarop de Wbp is gebaseerd.

Het gebruik van persoonsgegevens is noodzakelijk voor de bedrijfsprocessen van instellingen van onderwijs en onderzoek. Opslag en verwerking van deze persoonsgegevens dient met de grootste zorgvuldigheid te gebeuren, omdat misbruik van persoonsgegevens grote schade kan berokkenen aan studenten, medewerkers en Nyenrode.

Het College van Bestuur van NBU is wettelijk verantwoordelijk voor het op een juiste manier verwerken van persoonsgegevens. Met de maatregelen beschreven in dit beleidsdocument neemt NBU haar verantwoordelijkheid om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens te optimaliseren en daarmee te voldoen aan de relevante privacywet- en regelgeving.

Definities en afkortingen zijn te vinden in Bijlage A.

2.1 Reikwijdte en doelstelling van het privacy beleid

Het informatiebeveiligingsbeleid van Nyenrode beoogt de continuïteit van het bedrijfsproces te waarborgen, beveiligingsincidenten te voorkomen of de schade hiervan te minimaliseren, en tenminste te voldoen aan wet- en regelgeving.

Het privacy beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen NBU, waaronder in ieder geval alle medewerkers, studenten, gasten, bezoekers en externe relaties, alsmede op andere betrokkenen waarvan NBU persoonsgegevens verwerkt.

Bijzondere externe relaties zijn de accreditatie organisaties waarmee NBU gegevens uitwisselt om de onderwijskwaliteit meetbaar te maken, te borgen en extern te laten valideren. Dit betreft performance gegevens van studenten en deelnemers (met betrekking tot de kwaliteit van toetsing, afstudeerwerkstukken, diploma's en docenten). Maar bijvoorbeeld ook informatie over carrièreverloop en salariëring. Daar waar bijzonderheden gelden met betrekking tot het accreditatie proces, bijvoorbeeld het beheren van scripties onder embargo, in verband met concurrentie gevoelige informatie of anderszins hoog confidentiële inhoud, heeft het ASC de regie in het beschikbaar stellen van dergelijke documenten, ten behoeve van (in- en externe) audits.

Het privacy beleid betreft niet het verwerken van persoonsgegevens voor persoonlijk of huishoudelijk gebruik, zoals persoonlijke werkaantekeningen of een verzameling visitekaartjes. Het privacy beleid betreft de geheel of gedeeltelijk geautomatiseerde en/of systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van NBU alsmede de daaraan ten grondslag liggende (al dan niet elektronische) documenten. Eveneens is het privacy beleid van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens, die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Bij NBU wordt het beschermen van persoonsgegevens breed geïnterpreteerd. Er is een belangrijke relatie en gedeeltelijke overlap met het aanpalende beleidsterrein informatiebeveiliging, waarbij het gaat om de beschikbaarheid, integriteit en de vertrouwelijkheid van data, waaronder persoonsgegevens. Eveneens is het noodzakelijk om data opslag (intern en extern) te managen, om bijvoorbeeld te voorkomen dat NBU data buiten de EU wordt opgeslagen en beheerd door derden. Er wordt in het Nyenrode privacy beleid aandacht geschonken aan de raakvlakken met de informatie beveiliging en er wordt zowel planmatig als inhoudelijk afstemming gezocht.

Het privacy beleid heeft als doel om de kwaliteit van de verwerking en de beveiliging van persoonsgegevens permanent te verbeteren waarbij een zo optimaal mogelijke balans moet worden gevonden tussen privacy, functionaliteit en veiligheid.

Beoogd wordt de persoonlijke levenssfeer van de betrokkene zoveel mogelijk te respecteren. De gegevens, die betrekking hebben op een betrokkene dienen, op basis van het fundamenteel recht op bescherming van zijn/haar persoonsgegevens, beschermd te worden tegen onwettelijk en ongeautoriseerd gebruik, en tegen verlies dan wel misbruik. Dit brengt met zich mee dat het verwerken van persoonsgegevens dient te voldoen aan relevante wet- en regelgeving en dat persoonsgegevens veilig zijn bij NBU.

Het privacy beleid geeft studenten, medewerkers en andere betrokkenen inzicht in hoe privacy geregeld is op NBU. Daarnaast helpt het bij het creëren van bewustwording over het belang en de noodzaak van het beschermen van persoonsgegevens.

2.2 De belangrijkste punten van het privacy beleid:

- Het beleid vormt de start voor het managementsysteem en biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging te toetsen aan een vastgestelde norm en om de rollen inclusief taken, bevoegdheden en verantwoordelijkheden te beleggen;
- Voor de inrichting van het Nyenrode informatiebeveiligingsmanagement heeft ISO27001/2 als inspiratie gediend. Formele certificering conform ISO27001/2 wordt voor Nyenrode niet als noodzakelijk gezien, inrichting van een goed informatiebeveiligingsproces echter wel - dit beleid is daarvoor de basis;
- Maatregelen worden genomen op basis van gewijzigde wet- en regelgeving, een risicoanalyse en de uitkomsten van een audit;
- Uitgangspunten en organisatie van informatiebeveiligingsfuncties zijn expliciet vastgesteld en worden gedragen door het bestuur en afgeleid daarvan door de hele instelling;
- Daadkrachtige procesbenadering, duidelijke keuzen in maatregelen, actieve controle op beleidsmaatregelen en de uitvoering daarvan:
- Het beleid biedt de basis om te voldoen aan vigerende wetgeving.

3 Wet- en regelgeving

Bij NBU wordt op de volgende wijze omgegaan met relevante wet- en regelgeving.

Wet op het Hoger onderwijs en Wetenschappelijk onderzoek (WHW):
NBU heeft een kwaliteitszorgsysteem, waarin onder meer het zorgvuldig hanteren van gegevens in de studentenadministratie en het verwerken van studieresultaten is gewaarborgd. Daarnaast worden integriteitscodes voor wetenschappelijk onderzoek nageleefd en toegepast.

Wet Bescherming Persoonsgegevens (Wbp)/ Algemene verordening gegevensbescherming (Avg):
NBU heeft de wettelijke vereisten geïmplementeerd door middel van het privacy beleid. Persoonsgegevens worden in overeenstemming met de relevante wet- en regelgeving op behoorlijke wijze verwerkt, met in acht neming van transparantie (artikel 5 Avg), rechtmatigheid (artikel 6 Avg) en beveiliging. Hierbij dient een zo optimaal mogelijke balans te worden gevonden tussen het belang van NBU om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn/haar persoonsgegevens.

In het document 'Beleid verwerking persoonsgegevens 'Student' Nyenrode Business Universiteit', zijn de beleidsprincipes en de daarin voorkomende begrippen in hoofdstuk 4 uitgewerkt.

Archiefwet:
NBU stelt de voorschriften op ten aanzien van bewaartermijnen op basis van onder andere de Archiefwet en het Archiefbesluit.

Telecommunicatiewet:
NBU onderschrijft onder meer de regels waaraan cookies op websites dienen te voldoen.

Auteurswet:
NBU leeft het portretrecht na. Zij staat niet toe dat afbeeldingen, foto's en video's worden gepubliceerd wanneer een redelijk belang van de betrokkene zich daartegen verzet. Daarnaast stelt de Avg aanvullende eisen op het gebied van privacy gevoelige informatie verwerken. Zie voor het gebruik van afbeeldingen, 'Beleid verwerking persoonsgegevens 'Student' Nyenrode Business Universiteit' hoofdstuk 6.1.3.

Wet Computercriminaliteit:
Deze wet richt zich op de strafrechtelijke probleemgebieden in relatie tot computergebruik. De wet bestaat uit artikelen die op diverse plekken zijn toegevoegd aan het Wetboek van Strafrecht. De extra artikelen betreffen:

- Vernieling en onbruikbaar maken;
- Aftappen van gegevens;
- *Denial of service*, verstikkingsaanval;
- Computervredebreuk;
- Diensten afnemen zonder betalen;
- Malware, kwaadaardige software.

Wanneer er aanvallen op NBU plaatsvinden die die beveiliging significant doorbreken en die vallen onder de Wet Computercriminaliteit, zal NBU in beginsel aangifte doen. De regiegroep IBP adviseert hierover aan het bestuur– alleen het bestuur kan het besluit tot aangifte nemen.

4 Rollen en verantwoordelijkheden met betrekking tot verwerking persoonsgegevens

Om de verwerkingen van persoonsgegevens gestructureerd en gecoördineerd op te pakken is een aantal rollen en verantwoordelijkheden aan functionarissen in de bestaande organisatie toegewezen.

4.1 College van Bestuur

Het College van Bestuur (CvB) is eindverantwoordelijk voor de rechtmatige en zorgvuldige verwerking van persoonsgegevens binnen NBU en stelt het beleid, de maatregelen en de procedures op het gebied van verwerking met dit privacy beleid en onderliggende documenten vast.

4.2 Portefeuillehouder privacy

De portefeuillehouder privacy is het bestuurslid dat privacy in portefeuille heeft. Hij/zij is eindverantwoordelijk voor beveiliging van persoonsgegevens binnen NBU.

4.3 IT Security Manager

De IT Security Manager definieert de ICT-beveiligingsrichtlijnen voor de organisatie in overeenstemming met de informatiebeveiligingsstrategie en -architectuur van de organisatie en organiseert en coördineert de ICT-beveiliging van de organisatie. De IT Security Manager is de spin-in-het-web met betrekking tot informatiebeveiliging binnen de organisatie en vanuit deze hoedanigheid verantwoordelijk voor het aansturen van het Computer Emergency Response Team (CERT)-Nyenrode.

4.3.1 CERT-Nyenrode

Het CERT Nyenrode is een (virtueel) team dat bij elkaar wordt geroepen zodra zich een ernstig security incident heeft voorgedaan.

4.4 Functionaris voor de gegevensbescherming

De Functionaris voor de gegevensbescherming (FG) houdt binnen Nyenrode toezicht op de toepassing en naleving van de Wbp. De FG is in samenwerking met de IT Security Manager verantwoordelijk voor het afwikkelen van alle security-incidenten die betrekking hebben op de Wbp/Avg. Conform Avg heeft de FG een onafhankelijke positie in de organisatie.

De FG adviseert en informeert de gehele organisatie en de individuele eenheden omtrent het toepassen van de Privacy wetgeving. De FG draagt zorg voor de voorlichting over de verwerking van persoonsgegevens aan medewerkers, studenten en leidinggevenden. De FG bevordert het privacy bewustzijn van medewerkers en studenten, bijvoorbeeld door het onderhouden van een privacy portal op de website van NBU. Jaarlijks wordt er een privacy jaarverslag opgesteld.

De FG is aanspreekpunt en vraagbaak voor degenen die vragen hebben over de bescherming van persoonsgegevens en hij/zij beheert het register van meldingen van verwerkingen van persoonsgegevens.

De FG heeft de rol van procesmanager van het privacy incident proces. Dat houdt in dat hij/zij de universiteit brede inrichting van het proces bewaakt en verantwoordelijk is voor de kwaliteitszorg.

4.5 Proces/Systeemeigenaar

De proceseigenaar/systeemeigenaar is de persoon die de bevoegdheid heeft om te bepalen hoe een proces verloopt, en de verantwoordelijkheid heeft ervoor te zorgen dat het proces aan de klantverwachtingen en bedrijfsdoelstellingen blijft voldoen, vandaag en in de toekomst. Hierbij is de beveiliging van gerelateerde informatiesystemen van essentieel belang. In eerste instantie benoemt Nyenrode deze rol voor de meest vitale strategische bedrijfsfuncties Dit zijn: Customer Relationship Management, (CRM) systeem, Human Resource Management (HRM) systeem, Financieel Systeem, Camera systeem, Onderwijssysteem en de Website.

4.6 Leidinggevende

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft de taak om:

- ervoor te zorgen dat zijn medewerkers op de hoogte zijn van het beveiligingsbeleid;
- toe te zien op de naleving van het beveiligingsbeleid door zijn medewerkers;
- periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde informatiebeveiligingszaken.
- De leidinggevende kan hierin ondersteund worden door de FG.

Het verdient aanbeveling om een Privacy Contact Persoon (PCP) te benoemen.

4.7 Gebruiker

Iedere gebruiker wordt geacht de beveiligingsrichtlijnen en –procedures na te leven en op de hoogte te zijn van het beleid met betrekking tot privacy.

4.8 Onderzoeker

Iedere onderzoeker is verantwoordelijk voor de wijze waarop hij/zij onderzoekdata hanteert, in voorkomende gevallen samen met een onderzoeksleider; de hoogleraar of voorzitter van de onderzoeksgroep. Dit dient verder te worden uitgewerkt in het databeleid van NBU.

De privacy gevoeligheid en de ethische implicaties kunnen gevolgen hebben voor de opzet van het onderzoek en voor de wijze waarop met de onderzoekdata moet worden omgegaan. Het proportionaliteitsprincipe geeft aan dat de verwerking van persoonsgegevens proportioneel moet zijn aan het beoogde (onderzoek)doel. Het is aan de onderzoeker om deze afweging te maken.

4.9 Gelieerde instellingen

Aan NBU gelieerde instellingen, stichtingen en verenigingen zijn zelf verantwoordelijk voor het voldoen aan de Privacywetgeving. NBU zal het belang hiervan benadrukken en inzicht vragen in hoe compliance gerealiseerd is.

Gegevensverwerkingen van gelieerde instellingen kunnen niet gemeld worden bij de FG van NBU, maar dienen, voor zover zij niet binnen het Vrijstellingsbesluit[1] vallen, rechtstreeks bij de Autoriteit Persoonsgegevens (AP) gemeld te worden.

Voor advies kunnen gelieerde instellingen een beroep doen op de FG.

[1] Standaardverwerkingen die veel voorkomen waarvan algemeen bekend is dat zij plaatsvinden hoeven onder bepaalde voorwaarden niet gemeld te worden. Zie https://autoriteitpersoonsgegevens.nl/nl/melden/handreiking-vrijstellingsbesluit-wbp

5. Managementsysteem voor informatiebeveiliging

5.1 Overzicht managementsysteem informatiebeveiliging

Informatiebeveiligingsmanagement is als proces ingericht. Nyenrode kiest ervoor om de jaarlijkse planning en controlecyclus te baseren op “Plan, Do, Check, Act”. Hierin worden jaarlijks planningen gemaakt en uitgevoerd. De resultaten ervan worden geëvalueerd en vertaald naar nieuwe jaarplanningen. Deze planningen zullen als regel op strategisch niveau te vinden zijn in de Nyenrode planning, en meer in detail in de IT jaarplannen. Dit borgt een continu proces.

De samenhang tussen deze stappen is als volgt:

- Plan : Beleidsvorming en Risicoanalyse;
- Do : Planvorming en Implementatie;
- Check : Monitoring, evaluatie, controle en rapportage;
- Act : Het verbeterproces.

In de volgende paragrafen worden de stappen toegelicht.

5.2 Beleidsvorming

Het managementsysteem voor informatiebeveiliging begint met het opstellen van het informatiebeveiligingsbeleid. In dit beleid worden de doelstellingen en uitgangspunten voor informatiebeveiliging van Nyenrode vastgelegd. Hiermee vormt het beleid de leidraad voor de overige stappen van het managementsysteem.

5.3 Risicoanalyse

De tweede stap van het managementsysteem voor informatiebeveiliging bestaat uit een risicoanalyse. Het analyseren van risico’s heeft tot doel:

- Inzicht te krijgen in de kwaliteit en de effectiviteit van de bestaande beveiligingsmaatregelen;
- Inzicht te krijgen in de risico’s die de realisatie van het gewenste beveiligingsniveau in gevaar kunnen brengen;
- Het gewenste niveau van informatiebeveiliging vast te stellen in de vorm van een classificatie van bedrijfsprocessen, informatiesystemen en gegevensverzamelingen;
- Keuzes te kunnen maken voor het beheersen van risico’s;
- Prioriteiten te bepalen voor de verbetering van de bestaande situatie.

Over de uitkomsten van de analyse van de bestaande situatie voor informatiebeveiliging wordt gerapporteerd aan de regiegroep IBP.

5.4 Planning

Op basis van de uitkomsten van de risicoanalyse wordt een verbeterplan opgesteld. In dit plan worden de verbeteractiviteiten voor de realisatie van het gewenste beveiligingsniveau op projectmatige wijze vastgelegd. Het informatiebeveiligingsplan wordt vastgesteld door de regiegroep Informatiebeveiliging en Privacy (IBP).

5.5 Implementatie

Aan de hand van het verbeterplan wordt de implementatie van de aanvullende beveiligings- maatregelen ter hand genomen. Dit betekent onder andere het opstellen van richtlijnen en procedures voor informatiebeveiliging, het invoeren van maatregelen om de beveiliging op het gewenste niveau te krijgen en het voorlichten en opleiden van medewerkers.

5.6 Monitoren, evalueren, controleren en rapporteren

De laatste stap van het managementsysteem voor informatiebeveiliging bestaat uit monitoring, evaluatie en controle. Monitoring betreft het continu bewaken van het niveau van informatiebeveiliging binnen Nyenrode. Daar waar dit niveau in gevaar komt door het optreden van bedreigingen treedt incidentmanagement in werking om het gewenste beveiligingsniveau te waarborgen of zo snel mogelijk te herstellen. Nadat de bedrijfsfunctie hersteld is, vindt een evaluatie plaats met alle betrokkenen. Vervolgens wordt een rapport opgemaakt t.b.v. dossiervorming en bewustwording.

5.7 Continu proces

Het managementsysteem voor informatiebeveiliging omvat een continu en cyclisch proces. Dit betekent dat op basis van de uitkomsten van evaluaties en controles of door nieuwe ontwikkelingen (introductie van nieuwe bedrijfsprocessen of informatiesystemen) de noodzaak aanwezig kan zijn het informatiebeveiligingsbeleid te heroverwegen, een nieuwe risicoanalyse uit te voeren, extra maatregelen te treffen of de implementatie hiervan aan te passen. Nyenrode kiest om 1x per 2 jaar een audit + penetratietest [2] te laten uitvoeren waarbij de vorm per keer afzonderlijk wordt bekeken.

[2] Audit: een kort onderzoek naar de mate van informatieveiligheid in relatie tot de code van informatiebeveiliging en de Wbp /Avg

Penetratietest: een kwetsbaarheidsonderzoek (intern/extern gericht) op de IT infrastructuur om te veiligheid van informatie te controleren.

6. Implementatie privacy beleid

6.1 Verantwoordelijkheden

Het College van Bestuur is verantwoordelijk voor verwerkingen van de persoonsgegevens waarvan zij het doel en de middelen voor de verwerking vaststelt (zie hierboven hoofdstuk 4). Zij wordt aangemerkt als de *verantwoordelijke* in de zin van de wet. De feitelijke verwerking van persoonsgegevens wordt echter op allerlei plekken binnen de universiteit uitgevoerd. Een goede *governance* zorgt er voor dat alle belanghebbenden hun rechten en plichten kennen en er naar handelen.

Privacy is *ieders verantwoordelijkheid*. Van medewerkers, studenten, docenten en derden wordt verwacht dat ze zich integer gedragen en zorgvuldig omgaan met persoonsgegevens. Het is om deze reden dat er gedragscodes zijn geformuleerd en geïmplementeerd.

Privacy is *een lijnverantwoordelijkheid*. Dit betekent dat leidinggevenden de primaire verantwoordelijkheid dragen voor een zorgvuldige verwerking van persoonsgegevens op hun afdeling/eenheid. Dit omvat ook de keuze van de maatregelen, de uitvoering en de handhaving ervan. Onder de lijnverantwoordelijkheid valt ook de taak om het beleid met betrekking tot de verwerking van persoonsgegevens te communiceren met alle relevante partijen, binnen de grenzen van het redelijke.

6.2 Overleg

Om de samenhang in de organisatie van de informatiebeveiligingsfunctie goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van informatiebeveiliging binnen de verschillende onderdelen op elkaar af te stemmen wordt bij Nyenrode gestructureerd overleg gevoerd over het onderwerp informatiebeveiliging op diverse niveaus.

Op strategisch niveau wordt richtinggevend gesproken over governance en compliance, alsmede over doelen en ambitie op het gebied van informatiebeveiliging. Dit gebeurt in het bestuur, geadviseerd door de IT Security Manager en Functionaris Gegevensbescherming. Dit overleg vindt 1x per jaar plaats.

Op tactisch niveau wordt de strategie vertaald naar plannen, te hanteren normen, evaluatiemethoden, rapportages. Deze plannen en instrumenten zijn sturend voor de uitvoering. Dit tactisch overleg wordt uitgevoerd door de regiegroep IBP (eventueel in overleg met proceseigenaren). Dit overleg wordt ieder kwartaal gehouden en vaker indien hier aanleiding voor is.

Op operationeel niveau worden de zaken besproken die het dagelijkse bedrijfsproces aangaan in de zin van uitvoering en implementatie. Dit overleg met een ad-hoc karakter vindt onder andere plaats op het moment dat zich een informatie-beveiligingsincident voordoet. Hier wordt de oplossingsrichting bepaald en worden de verschillende taken verdeeld.

Het verwerken van persoonsgegevens is een continu proces. Technologische en Organisatorische ontwikkelingen binnen en buiten NBU maken het noodzakelijk om periodiek te bezien of NBU nog voldoende op koers zit met het beleid.

6.3 Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Het is noodzakelijk om bij medewerkers en studenten het bewustzijn m.b.t. privacy en security voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en goed gedrag wordt aangemoedigd. Good practices kunnen gedeeld worden met anderen in de organisatie, bijvoorbeeld via de privacy portal op de website van NBU.

Onderdeel van de uitvoering van het privacy beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, studenten en derden. Deze campagnes kunnen aansluiten bij landelijke campagnes in het hoger onderwijs, zo mogelijk in afstemming met andere beveiligingscampagnes.

6.4 Controle en naleving

De FG houdt toezicht op de naleving van de privacywetgeving en het privacy beleid, inclusief de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van personeel. Aanvullend hierop maken audits het mogelijk het privacy beleid en de genomen maatregelen te controleren op effectiviteit.

Mocht de naleving op de bescherming van data- en privacygegevens ernstig tekort schieten, dan kan NBU de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de wettelijke mogelijkheden.

7. Rechtmatige en zorgvuldige verwerking van Persoonsgegevens

7.1 Grondslag, doelbinding en belangenafweging

Het verwerken van persoonsgegevens moet gebaseerd zijn op wettelijke gronden zoals beschreven in artikel 8 van de Wbp en artikel 6 van de Avg. De verantwoordelijke omschrijft vooraf de doeleinden voor de verwerking. Deze doeleinden zijn concreet en specifiek geformuleerd. Bij elke verwerking wordt getoetst in hoeverre het verwerken van persoonsgegevens noodzakelijk is. Hierbij worden de verschillende belangen afgewogen en wordt gekeken naar de doelmatigheid, proportionaliteit en subsidiariteit. persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.

NBU treft de nodige maatregelen om te zorgen dat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, juist en nauwkeurig zijn.

7.2 Melden en documenteren van verwerkingen

Een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens dient gemeld te worden bij de FG van NBU. De FG beoordeelt de rechtsgeldigheid van de registratie en draagt zorg voor adequate documentatie.

De verwerkingen worden voldoende gedocumenteerd en gepubliceerd op voor de betrokkenen toegankelijke media met vermelding van het doel van de registratieregistraties en de verantwoordelijken.

7.3 De organisatie van de beveiliging

NBU draagt zorg voor een adequaat beveiligingsniveau en legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen zijn er mede op gericht onnodige c.q. onrechtmatige verzameling en verwerking van persoonsgegevens te voorkomen.

Bij (onderzoeks)projecten, infrastructurele wijzigingen of de aanschaf van nieuwe systemen, wordt vanaf de start rekening gehouden met de inrichting van privacy door een Privacy Impact Assessment (PIA) uit te voeren. De FG wordt geconsulteerd bij dergelijke wijzigingen. Twee principes zijn richtinggevend:

1. Gedurende het beheer van de gehele levenscyclus van persoonsgegevens, vanaf het verzamelen tot het verwerken en verwijderen, wordt stelselmatig aandacht besteed aan allesomvattende waarborgen m.b.t. nauwkeurigheid, vertrouwelijkheid, integriteit, fysieke veiligheid en verwijdering van de persoonsgegevens.
2. Wanneer gebruikers de keuze wordt geboden tussen verschillende opties, dan geeft de standaard instelling de beste privacy garanties.

Een risicoanalyse op privacybescherming en informatiebeveiliging maakt deel uit van het intern risicobeheersings- en controlesysteem van NBU.

7.4 Geheimhouding

Bij NBU worden alle persoonsgegevens als vertrouwelijk geclassificeerd. Een ieder behoort de vertrouwelijkheid van persoonsgegevens te kennen en daarnaar te handelen.

Ook personen voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennis nemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

7.5 Bewaartermijnen / vernietigingstermijnen per soort gegeven

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de doeleinden waarvoor zij zijn verzameld of worden gebruikt. Persoonsgegevens dienen na het verlopen van de bewaartermijn[3] buiten het bereik van de actieve administratie gebracht te worden. NBU zal de persoonsgegevens na het verlopen van de bewaartermijn op correcte wijze laten vernietigen of, indien de persoonsgegevens bestemd zijn voor historische, statistische of wetenschappelijke doeleinden, in een archief bewaren.

7.6 Bijzondere Persoonsgegevens

Het verwerken van bijzondere persoonsgegevens is in beginsel verboden, tenzij er sprake is van een wettelijke grondslag, uitdrukkelijke toestemming van de betrokkene of een zwaarwegend algemeen belang. Er gelden zwaardere eisen voor de beveiliging van deze persoonsgegevens. Daar waar de basisbescherming niet voldoende is, moeten voor elk informatiesysteem individueel afgestemde extra maatregelen worden genomen. Zie voor het verwerken van persoonsgegevens in de dagelijkse onderwijs administratie praktijk het document, ‘Beleid verwerking persoonsgegevens ‘Student’ Nyenrode Business Universiteit’.

7.7 Doorgifte persoonsgegevens aan derden

7.7.1 Uitbesteden van verwerking aan een bewerker

Indien NBU persoonsgegevens laat verwerken door een bewerker, wordt de uitvoering van verwerkingen geregeld in een schriftelijke overeenkomst tussen NBU, zijnde de verantwoordelijke en de bewerker. Ook wanneer NBU bewerker is voor een externe partij, bijvoorbeeld door maatwerk onderwijs in opdracht te leveren, worden de verwerkingen van persoonsgegevens contractueel overeengekomen en vastgelegd.

7.7.2 Doorgifte persoonsgegevens binnen de Europese Unie

NBU verstrekt persoonsgegevens alleen aan derden binnen de EU, als deze doorgifte is gebaseerd op een wettelijke grondslag.

Met betrekking tot bijzondere persoonsgegevens worden deze niet aan derden verstrekt zonder expliciete toestemming van de betrokkene.

[3] Bewaartermijnen kunnen wettelijk zijn bepaald, zoals bij financiële gegevens of formele studieresultaten, maar kunnen ook zijn vastgelegd door de NBU b.v. in een bewerkersovereenkomst tussen NBU en de Betrokkenen.

7.7.3 Doorgifte persoonsgegevens buiten de Europese Unie

NBU verstrekt persoonsgegevens alleen aan derden, die zich bevinden in een land buiten de Europese Unie, indien dat land in zijn geheel of dat bedrijf/die instelling specifiek een passend *beschermingsniveau waarborgt*. Voor landen met een passend beschermingsniveau hanteert NBU de lijst van landen, zoals gepubliceerd door de Europese Commissie[4].

NBU verstrekt persoonsgegevens alleen aan landen zonder passend beschermingsniveau op basis van een wettelijke uitzondering zoals genoemd in artikel 77 van de Wbp of op grond van de overwegingen genoemd in onder 104) en 107) van de Avg. Eén van die uitzonderingen is “ondubbelzinnige toestemming”: degene van wie persoonsgegevens doorgegeven wordt, heeft ondubbelzinnige toestemming gegeven. Een andere wettelijke uitzondering is doorgifte op basis van een modelcontract (zoals opgesteld door de Europese Commissie). Bij wijzigingen van of aanvullingen op het modelcontract is een vergunning van de minister van Veiligheid en Justitie vereist. In alle gevallen is bij doorgifte van persoonsgegevens aan een land buiten de Europese Unie een melding bij de Autoriteit Persoonsgegevens verplicht.

Derden aan wie NBU persoonsgegevens doorgeeft (niet limitatieve lijst):

- DUO;
- Overheidsinstellingen;
- Gemeenten;
- Belastingdienst;
- Stagebedrijven/organisaties;
- Accreditatie organisaties;
- Studieverenigingen;
- Studentenverenigingen.

[4] Zie voor deze lijst: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal-gegevensverkeer/doorgifte-binnen-en-buiten-de-eu#wanneer-mag-ik-toch-persoonsgegevens-doorgeven-naar-een-derde-land-zonder-passend-beschermingsniveau-1753

8. Privacy regels

Op deelgebieden zijn specifieke privacy regels noodzakelijk. Medewerkers kunnen zich beperken tot de voor hen relevante privacy regels. Door het formeel vaststellen van deze privacy regels wordt de implementatie van het privacy beleid toetsbaar.

Voor de volgende deelgebieden zijn specifieke privacy regels vastgesteld:

1. *Inventarisatie van gegevensverwerkingen;*
2. *Website en Apps;*
3. *Wetenschappelijk onderzoek;*
4. *Administratie en bedrijfsvoering;*
5. *Cameratoezicht;*
6. *Aandachtspunten vertrouwelijkheid.*

8.1 Privacy regels – Inventarisatie Gegevensverwerkingen

Inleiding

In het privacy beleid wordt aangegeven dat er op deelgebieden specifieke privacy regels noodzakelijk zijn. Een van deze deelgebieden betreft de inventarisatie van gegevensverwerkingen.

Verantwoordelijkheid

1. Gegevensverwerkingen worden volgens artikel 27 Wbp en Avg artikel 30 gemeld bij de FG;
2. De proceseigenaar draagt zorg voor deze melding;
3. De FG draagt zorg voor de inventarisatie van de meldingen van de gegevensverwerkingen.

Meldingen

Iedere melding bevat tenminste de volgende gegevens:

- Functionele naam van het systeem;
- Houder van het systeem;
- Betrokken externe partijen;
- Doel van de verwerking;
- Welke categorieën van persoonsgegevens van welke categorieën van betrokkenen worden vastgelegd;
- Te hanteren bewaartermijnen, dit kan per soort gegeven verschillen;
- Welke bijzondere persoonsgegevens[5] worden vastgelegd;
- Beschrijving van de genomen beveiligingsmaatregelen;
- Lijst van organisaties aan wie persoonsgegevens worden verstrekt.

Bij het doel van de verwerking wordt ook de wettelijke grondslag vermeld:

- Toestemming van de betrokkene;
- Uitvoeren van een overeenkomst;
- Een wettelijke verplichting;
- Ter vrijwaring van een vitaal belang van de betrokkene;
- Uitvoering van een publiekrechtelijke taak;
- Gerechtvaardigd belang van de verantwoordelijk of derde aan wie gegevens zijn verstrekt;
- De FG draagt zorg voor de kwaliteitscontrole van de meldingen;
- Informatiesystemen die geen persoonsgegevens gebruiken worden niet gemeld.

Verwerkingen die onder het Vrijstellingsbesluit[6] vallen, worden ten behoeve van het overzicht toch zoveel mogelijk gemeld bij de FG.

Transparantie

Een overzicht van de meldingen wordt door de FG gepubliceerd op de website.

[5] De verwerking van persoonsgegevens betreffende iemands godsdienst of levensovertuiging, gender identiteit, ras, politieke gezindheid, gezondheid, seksuele leven, vakbondslidmaatschap en strafrechtelijke gegevens is alleen toegestaan onder bepaalde voorwaarden, Wbp paragraaf 2, Avg artikel 9.

[6] Standaardverwerkingen die veel voorkomen waarvan algemeen bekend is dat zij plaatsvinden hoeven onder bepaalde voorwaarden wettelijk gezien niet gemeld te worden. Vrijstellingsbesluit Wbp, *stb*. 2014, 520 (in werking getreden op 7 mei 2001), zie http://wetten.overheid.nl/BWBR0012461 Aangezien de NBU wel een overzicht wil hebben van alle verwerkingen is een interne melding wel gewenst.

8.2 Privacy regels – Website en apps

Inleiding

In het privacy beleid wordt aangegeven dat er op deelgebieden specifieke privacy regels noodzakelijk zijn. Een van deze deelgebieden betreffen de websites en apps van NBU.

Verantwoordelijkheid

1. M&C is verantwoordelijk voor de implementatie van het privacy beleid op de websites en in apps;
2. Websites op sub domeinen vallen onder de verantwoordelijkheid van de betreffende eenheid of vereniging. M&C geeft hen proactief advies;
3. M&C informeert website-beheerders over de relevante privacy regels wanneer deze met formulieren persoonlijke informatie verzamelen.

Volgen van bezoekers

1. Bezoekers worden alleen gevolgd voor zover daar een goede reden voor is, hierbij wordt het proportionaliteitsprincipe toegepast;
2. Op de websites en in apps wordt duidelijk aangegeven hoe en met welk doel bezoekers gevolgd worden;
3. Op de websites en in apps wordt duidelijk vermeld welke gegevens worden verzameld;
4. Op de websites en in apps wordt duidelijk aangegeven hoe bezoekers de website kunnen bezoeken of de app kunnen gebruiken zonder gevolgd te worden.

Formulieren

- Formulieren op de websites en in apps vragen niet meer persoonlijke informatie dan nodig is voor het doel waarvoor deze verzameld wordt;
- Ieder formulier maakt duidelijk voor welk doel of welke doelen de gevraagde informatie gebruikt wordt;
- Ieder formulier maakt deel uit van een informatiesysteem waarop de Privacy regels – Inventarisatie Gegevensverwerkingen van toepassing zijn.

IP-adressen

- IP-adressen worden niet gebruikt om bezoekers te volgen;
- IP-adressen worden gelogd en kunnen gebruikt worden om security-incidenten en/of technische storingen op te lossen;
- IP-blokken kunnen gebruikt worden voor statistische analyses.

8.3 Privacy regels – Wetenschappelijk onderzoek

Inleiding

In het privacy beleid wordt aangegeven op welke deelgebieden specifieke privacy regels noodzakelijk zijn. Eén van deze deelgebieden betreft het wetenschappelijk onderzoek. Onderzoekers hebben graag een helder overzicht van de voor hen relevante privacy regels, dit overzicht wordt hieronder gegeven. Deze regels gelden ook voor studenten, die met onderzoek bezig zijn.

Wanneer een faculteit een ethische commissie heeft dan wordt geadviseerd de PCP in het reviewproces te betrekken.

Relevante documenten

- Iedere onderzoeker die met persoonsgegevens werkt, dient kennis te nemen van de VSNU Gedragscode voor gebruik van persoonsgegevens in wetenschappelijk onderzoek[7];
- Iedere onderzoeker die met medische gegevens werkt, dient kennis te nemen van de Federa Gedragscode Gezondheidsonderzoek.[8]

Aanvang onderzoek

- Conform het Onderzoeksdatabeleid wordt een datamanagementplan opgesteld;
- Wanneer identificerende gegevens van personen worden gebruikt wordt conform de Privacy regels – Inventarisatie Gegevensverwerkingen in samenspraak met de PCP een melding gedaan bij de FG;
- Denk na over het anonimiseren of als dat niet mogelijk is pseudonimiseren van gegevens[9];
- Er worden heldere afspraken gemaakt hoe met persoonsgegevens wordt omgegaan. Dit wordt vastgelegd in het datamanagementplan.

Dataopslag

- Wanneer gebruik wordt gemaakt van externe opslag of andere clouddiensten dan wordt er een bewerkersovereenkomst[10] afgesloten;
- Bedenk dat persoonsgegevens niet zo maar buiten de EU opgeslagen mogen worden;
- Voorkom datalekken door zorgvuldig met dataopslag om te gaan;
- Wanneer vertrouwelijke informatie wordt vervoerd (bijvoorbeeld op een USB-stick of laptop) dan wordt versleuteling toegepast;
- Wanneer vertrouwelijke informatie aan anderen wordt verstrekt (bijvoorbeeld via een clouddienst of per email) dan wordt versleuteling toegepast;
- Voor toegang tot een data repository wordt het autorisatiebeleid toegepast.

[7] zie http://www.vsnu.nl/code-pers-gegevens.html
[8] zie https://www.federa.org/code-goed-gedrag
[9] artikel 89 lid 1 Avg: … Wanneer die doeleinden kunnen worden verwezenlijkt door verdere verwerking die de identificatie van betrokkenen niet of niet langer toelaat, moeten zij aldus worden verwezenlijkt.
[10] ASC kan hier ondersteuning bij bieden.

8.4 Privacy regels – Administratie en bedrijfsvoering

Inleiding

In het privacy beleid wordt aangegeven dat er op deelgebieden specifieke privacy regels noodzakelijk zijn. Een van deze deelgebieden betreft de administratie en bedrijfsvoering. De privacyregels (zie hoofdstuk 8.6) –zijn onverkort van toepassing op de administratie en bedrijfsvoering.

Verantwoordelijkheid

De houder of eigenaar van een informatiesysteem is verantwoordelijk voor naleving van de privacy regels.

Verwerving

1. Voor of aan het begin van het project wordt er conform de Classificatierichtlijn Informatie en Informatiesystemen een classificatie uitgevoerd, zodat de resultaten de vereisten voor het informatiesysteem kunnen meebepalen;
2. Bij het gebruik van cloud-services wordt het Juridisch normenkader cloud-services hoger onderwijs van SURF toegepast;
3. Indien persoonsgegevens worden verwerkt dan wordt een Privacy Impact Assessment (PIA) uitgevoerd. De resultaten hiervan worden verwerkt in de business case voor het project. Er wordt getoetst in hoeverre het verwerken van persoonsgegevens noodzakelijk is. Hierbij worden de verschillende belangen afgewogen;
4. Idealiter is de FG bij de uitvoering van de PIA aanwezig/betrokken. In ieder geval wordt het resultaat aan de FG ter toetsing toegestuurd;
5. Indien een externe bewerker wordt ingeschakeld, wordt een bewerkersovereenkomst afgesloten.

Implementatie

1. Vanaf het begin van het ontwerpproces wordt met privacy rekening gehouden en wordt dataminimalisatie toegepast;
2. De houder meldt de gegevensverwerking bij de FG voordat het systeem in gebruik wordt genomen;
3. Bewaartermijnen worden vastgelegd, zodat persoonsgegevens niet langer worden bewaard dan noodzakelijk is;
4. Betrokkenen worden door de houder geïnformeerd over de gegevensverwerking;
5. De houder richt een proces in zodat tijdig, binnen vier weken, aan het recht op inzage en het recht op verbetering, aanvulling, verwijdering of afscherming voldaan kan worden;
6. Voor testdoeleinden worden in principe geen productiegegevens gebruikt, behalve voor het reproduceren van geconstateerde problemen. Wanneer voor een acceptatietest productiegegevens worden gebruikt, dan dient de autorisatiematrix gelijk te zijn aan die van de productieomgeving.

8.1 Privacy regels – Cameratoezicht

Inleiding

Voor het cameratoezicht op NBU zijn buiten de privacy regels de hieronder opgenomen regels van toepassing.

Verantwoordelijkheid
De proces- en systeemeigenaar Facilitair is verantwoordelijk voor het naleven van de privacyregels bij het cameratoezicht op NBU onder eindverantwoordelijkheid van het CvB.

Doel en transparantie
De gegevens worden uitsluitend gebruikt voor de volgende doeleinden:

- Bescherming van de veiligheid en gezondheid van natuurlijke personen;
- Beveiliging van de toegang tot gebouwen en terreinen*;
- Bewaking van zaken die zich in gebouwen of op terreinen bevinden;
- Vastleggen van incidenten.

Camera's zijn duidelijk zichtbaar opgehangen of er wordt ter plekke, bijvoorbeeld middels borden, aangegeven dat gebruik wordt gemaakt van camerabewaking.

Toegang

- De live beelden zijn alleen toegankelijk voor de medewerkers die belast zijn met de beveiliging en bewaking op NBU;
- Toegang tot opgenomen beelden is alleen mogelijk in een speciaal daartoe ingerichte ruimte;
- Toegang tot opgenomen beelden hebben alleen het hoofd van de verantwoordelijke afdeling en diens plaatsvervanger;
- Betreffende medewerkers hebben een geheimhoudingsplicht met betrekking tot gegevens die tot personen herleidbaar zijn.

Opslag

- Opgenomen camerabeelden worden zo opgeslagen dat deze niet toegankelijk zijn voor anderen;
- Opgenomen camerabeelden worden niet langer dan twee weken bewaard.

Beheer beeldgegevens

Het CvB, de ondernemingsraad en de Functionaris Gegevensverwerking (FG) ontvangen jaarlijks een overzicht van de actuele cameratoepassingen. Hierin staat de locatie van de camera's vermeld, de toepassing ervan en wordt aangegeven voor welke medewerkers de monitoren en eventueel opgeslagen beelden toegankelijk zijn. Indien er een uitbreiding van het cameratoezicht plaatsvindt, de toepassing van een camera gewijzigd of een camera verwijderd wordt, zal de proces- en systeemeigenaar Facilitair, de OR en de FG vooraf om instemming worden gevraagd.

*Dit betreft niet de handhaving van de openbare orde zoals bepaald in artikel 151c van de Gemeentewet.

Incidenten
NBU heeft een gedragscode waarin (ongeoorloofd) gedrag is beschreven. Camera's worden niet actief ingezet om gedrag te monitoren. Echter, na een incident kan, als blijkt dat relevant beeldmateriaal beschikbaar is, wel besloten worden deze beelden veilig te stellen en zo lang te bewaren als voor een mogelijk intern onderzoek nodig is.

Beelden worden alleen aan derden verstrekt indien het belang van NBU dit vordert en alleen na een overeenkomstig besluit door het College van Bestuur. De politie kan de beelden alleen op vordering verkrijgen, of ná toestemming van de (hulp)officier van justitie.

8.2 Privacy regels – Aandachtspunten vertrouwelijkheid

Hieronder staan concrete generieke aandachtspunten op een rij, die per gegevensverwerkend proces vertaald moeten worden door houders van informatie systemen om al dan niet additionele maatregelen in te bouwen

Autorisatie. Het is van belang zeker te zijn dat alleen die personen toegang hebben tot vertrouwelijke informatie die die gegevens ook nodig hebben. Implementatie van het autorisatiebeleid kan hiervoor zorgdragen. Attent zijn op het gebruik van een account van een ander, ook bij tijdelijke vervanging zoals bv. bij zwangerschapsverlof.

Authenticatie. Voorkomen dat iemand zich voor iemand anders kan uitgeven en bij vertrouwelijke informatie kan komen. Voorkom dat medewerkers wachtwoorden delen of opschrijven. Overweeg twee factor authenticatie.

Toegang van elders dan de vaste werkplek. Thuiswerken of werken op een andere locatie kan tot extra risico's leiden. Dit is te voorkomen door te filteren op IP-adres.

Invoer van gegevens. Bedenk dat aantekeningen en tijdelijke documenten ook vertrouwelijke informatie kunnen bevatten. Zorg voor gecontroleerde afvoer of vernietiging van dergelijke papieren en bestanden.

Bewerken en raadplegen van gegevens. Wanneer een medewerker informatie opvraagt of toevoegt, kan vertrouwelijke informatie, als deze niet noodzakelijk is voor de handeling, worden verborgen of achter een extra knop gezet worden.

Onderbreken van het werk. Denk om het gebruik van screensavers en om het niet zichtbaar laten liggen van vertrouwelijke papieren.

Uitwisselen gegevens met andere systemen. Wissel niet meer gegevens uit dan noodzakelijk. Wanneer vertrouwelijke informatie wordt verstrekt, wees er dan zeker van dat die gegevens ook vertrouwelijk blijven. Maak duidelijke afspraken vooraf.

Produceren van rapportages. Per rapport zal bepaald moeten worden welke mate van vertrouwelijkheid er moet gelden. Wanneer bekend is dat een rapport vertrouwelijk is, dan kan dat er standaard op vermeld worden.

Opslaan van gegevens. Kritiek vertrouwelijke informatie hoort versleuteld opgeslagen te worden. Bij centrale opslag is dat van belang om te voorkomen dat hackers of beheerders toegang hebben. Bij decentrale opslag speelt meer het risico van virussen en diefstal. Papier met kritiek vertrouwelijke informatie, bijvoorbeeld een dossier, dient opgeslagen te worden in een afgesloten kast.

Bewaren van email. Het bewaren van vertrouwelijke informatie in het emailsysteem betekent dat deze informatie via ieder device, dus ook de telefoon en tablet, langdurig toegankelijk blijft. Denk bijvoorbeeld aan ziektemeldingen, sollicitatiebrieven en functioneringsgesprekken. Verwijder e-mails met vertrouwelijke informatie zo snel mogelijk.

Archiveren van informatie. Leg de bewaartermijn en de regels omtrent toegang en vernietiging vast.

Afdrukken van gegevens. Papier met kritiek vertrouwelijke informatie mag alleen geprint worden als de medewerker er zelf bijstaat, mag niet blijven rondslingeren, mag niet zomaar meegenomen worden en moet na gebruik gecontroleerd afgevoerd of vernietigd worden.

Meenemen van digitale gegevens. Informatie kan op USB-stick, harde schijf, laptop, etc. meegenomen worden. Bedenk eerst of alle informatie wel nodig is, kan de vertrouwelijke informatie niet weggelaten worden? Kritiek vertrouwelijke informatie hoort versleuteld opgeslagen te worden.

Raadplegen van informatie op mobiele apparatuur. Zoals beschreven in de notitie Gebruik van “eigen” apparatuur en applicaties kunnen afhankelijk van de classificatie extra beveiligingsmaatregelen worden getroffen.

Werken in publieke ruimtes. Andere personen kunnen van scherm of papier meelezen. Voorkom dit bij het raadplegen van vertrouwelijke informatie. Denk hierbij aan gang, kantine, cafés, restaurants, wachtruimtes, trein, vliegtuig, etc.

Bespreken van informatie. Bedenk bij het bespreken van informatie, ook bij het gebruik van een telefoon, dat anderen mee kunnen luisteren.

Versturen van informatie. Controleer of de betreffende persoon deze informatie wel nodig heeft, probeer de verstrekte informatie te minimaliseren. Controleer of we als NBU deze informatie wel aan betreffende persoon mogen verstrekken. Wanneer vertrouwelijke informatie per email of anderszins digitaal verstuurd wordt, dan dient dit versleuteld te gebeuren.

Audittrail. Door middel van een logfile moet na te gaan zijn wie toegang tot welke vertrouwelijke informatie heeft gehad.

Diefstal van informatie. Wanneer papier met vertrouwelijke informatie of een informatiedrager (USB-stick, tablet, etc.) wordt verloren, welke procedures gelden er dan? Enerzijds minimaliseren verdere schade, door wachtwoord aan te passen etc.. Wat verder te doen wordt verder in de procedure Meldplicht Datalekken uitgewerkt.

Schrijven van procedures. Neem de rollen van medewerkers op in procedures en niet de namen van individuen.

Uitbreiden of nieuw ontwerpen/aanschaffen van applicaties. Bedenk vooraf welke beveiligingsaspecten een rol spelen. De Classificatierichtlijn en een PIA kunnen hierbij helpen. Halverwege een project met extra eisen komen zorgt voor hogere kosten.

Testen van applicaties. Voor het testen van een applicatie wordt vaak met de live-data gewerkt, die is immers realistisch. Maar voor de meeste tests kan de kritiek vertrouwelijke informatie prima weggelaten worden. Dit kan door bepaalde velden in een database met andere informatie te overschrijven of te verhaspelen en geen originele vertrouwelijke documenten te gebruiken.

Uitbesteden van werk of gebruik van clouddiensten. Maak heldere afspraken en als er persoonsgegevens worden uitgewisseld sluit dan een bewerkersovereenkomst af.

9 Incidenten met betrekking tot persoonsgegevens

Iedere klacht of melding met betrekking tot de verwerking van persoonsgegevens binnen NBU is een privacy incident. De bekendste vorm van zo'n incident is een datalek[11]. Dit hoofdstuk beschrijft het beleid met betrekking tot de melding, registratie en afhandeling van incidenten of het vermoeden van incidenten in de reguliere bedrijfsvoering en in bijzondere omstandigheden.

9.1 Melding en registratie

Medewerkers van NBU zijn verplicht om een (vermoedelijk) 'datalek' en andere privacy incidenten direct te melden bij de ICT Helpdesk (0346-291288 of helpdesk@nyenrode.nl). Indien de melder daar de voorkeur aan geeft kan dit ook vertrouwelijk bij de FG, deze zal de naam van de melder vertrouwelijk behandelen. Voorbeelden van datalekken staan in Bijlage C.

Van elk incident en de afhandeling daarvan wordt door ICT Services een registratie bijgehouden. Meldingen worden vertrouwelijk behandeld. De melder kan er op vertrouwen dat het doen van een melding geen persoonlijke consequenties heeft voor de melder. Een melder dient zolang het incident nog niet is afgehandeld vertrouwelijk met de melding om te gaan en hierover niet te communiceren met betrokkenen of anderen.

9.2 Afhandeling

Nadat de melding is ontvangen vindt een grondige analyse plaats om de omvang en impact te bepalen. Bij ernstige security incidenten wordt het Computer Emergency Response Team (CERT) Nyenrode geactiveerd. In de praktijk is dit een virtueel team dat bestaat uit de medewerkers van de dienst ICT. Meer informatie over de procesgang is te vinden op het centrale platform van Nyenrode; https://my.nyenrode.nl/organization1/Informatiebeveiliging/Pages/default.aspx

De afhandeling van incidenten heeft als doel het probleem op te lossen, de schade te beperken en de wetgeving na te leven. De incidenten worden afgehandeld en worden in het relevante operationeel overleg besproken – en als bedrijfsproces, financiën of goede naam in gevaar zijn, ook in het CvB. Bij constatering van verontrustende trends kan hierop meteen worden ingespeeld, bijvoorbeeld door het nemen van extra maatregelen of een bewustwordingscampagne.

Het doel van CERT-Nyenrode is het zo mogelijk voorkomen van informatiebeveiligings-incidenten en deze te bestrijden zodra ze zich voordoen en daarmee de continuïteit van Nyenrode te ondersteunen en haar reputatie te beschermen. CERT-Nyenrode houdt zich ook bezig met beveiligingsincidenten buiten Nyenrode als daar eigen medewerkers in enige rol bij betrokken zijn.

De leden van CERT-Nyenrode zijn benoemd door het Hoofd ICT en opereren in diens opdracht. CERT-Nyenrode kan in geval van ernstige incidenten via de IT Security Manager escaleren naar de portefeuillehouder informatiebeveiliging. Deze constructie maakt directe escalatie naar het CvB mogelijk evenals directe contacten met andere personen binnen Nyenrode die zorgdragen voor contacten met de pers en voor juridische zaken.

CERT-Nyenrode is gerechtigd het tijdelijk isoleren van systeem/netwerkgebruikers, computersystemen of netwerksegmenten te gelasten ten einde haar taak uit te kunnen voeren.

[11]Als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben, spreken we van een datalek.

De IT Security Manager beoordeelt of er sprake is van een datalek. Is dat het geval, dan wordt de FG betrokken bij de verdere afhandeling. Vaak zal ook de leidinggevende betrokken worden. De FG is verantwoordelijk voor de afhandeling van privacy incidenten. Als het incident een datalek betreft dan wordt conform de regels van de AP[12] bepaald of melding aan de AP verplicht is. De melding wordt afgestemd met het CvB. Een melding aan de AP dient uiterlijk 72 uur na de constatering plaats te vinden.

Wanneer het informeren van betrokkenen verplicht is conform de regels van de AP of anderszins gewenst is, wordt de communicatie in samenspraak met M&C verzorgd. De melder wordt geïnformeerd over de afhandeling van het incident.

9.3 Evaluatie

Het is van belang om te leren van incidenten. Naast het opstellen van een (beleid)visie, waarna deze wordt uitgewerkt in plannen en activiteiten om de gedefinieerde doelstellingen te kunnen behalen, moet het resultaat worden gemeten. Registratie van incidenten en een periodieke rapportage zijn daarbij een voorwaarde. Niet alleen kan dan worden gemeten of de activiteiten die ervoor moeten zorgen dat het resultaat bereikt wordt, worden uitgevoerd. Maar ook om zicht te krijgen op verdere verbeter punten. De rapportage over incidenten met betrekking tot persoonsgegevens maakt een vast onderdeel uit van het privacy jaarverslag en van de PDCA-cyclus.

[12] De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp). Beleidsregels voor toepassing van artikel 34a van de Wbp en Avg Artikelen 33 en 34; Overwegingen 85 tot en met 87.
Zie https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken

Bijlage A Definities en afkortingen

AP: Autoriteit Persoonsgegevens.

Avg: Algemene verordening gegevensbescherming. Verordening (EU) 2016/679. De Europese opvolger van de Wbp die vanaf mei 2018 van toepassing is.

Betrokkene: een individueel en natuurlijk persoon op wie een persoonsgegeven betrekking heeft.

Bewerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

CBP: College Bescherming Persoonsgegevens, de oude naam van de AP.

CvB: College van Bestuur.

Datalek: Persoonsgegevens die in handen vallen van derden die geen toegang tot die gegevens (mogen) hebben.

Derde: Ieder ander, niet zijnde de betrokkene, de verantwoordelijke of de bewerker, of enig persoon die onder rechtstreeks gezag valt van de verantwoordelijke of de bewerker en gemachtigd is om persoonsgegevens te verwerken.

FG: Functionaris voor de Gegevensbescherming.

PCP: Privacy Contact Persoon

Persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijk persoon.

Privacy Impact Assessment/Gegevensbeschermingseffectbeoordeling: Een hulpmiddel dat helpt bij het identificeren van privacy risico's en de handvaten levert om deze risico's te verkleinen tot een acceptabel niveau.

NBU: Nyenrode Business Universiteit, Universiteit Nyenrode B.V., Nyenrode.

Verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Op NBU is het CvB verantwoordelijk, maar dit is gedelegeerd aan de houder van het betreffende informatiesysteem.

Verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Wbp: Wet bescherming persoonsgegevens. Gebaseerd op Richtlijn 95/46/EG.

Bijlage B Classificatie

Voor het goed functioneren van de bedrijfsprocessen binnen Nyenrode is het juist omgaan met informatie van levensbelang. Studenten en medewerkers moeten er op kunnen vertrouwen dat informatie veilig; toegankelijk; beschikbaar; correct en volledig is. Bovendien mag informatie alleen beschikbaar zijn voor daartoe rechthebbende personen. Nyenrode is voornemens om alle gegevens, waarop dit informatiebeveiligingsbeleid van toepassing is te classificeren op de kwaliteitsaspecten *Beschikbaarheid*, *Integriteit* en *Vertrouwelijkheid*. Deze actie wordt opgenomen in het informatiebeveiligingsplan 2017 -2018.

B = Beschikbaarheid	Is de informatie/functie aanwezig/bruikbaar/leesbaar?
I = Integriteit	Is de informatie/functie betrouwbaar/compleet/onaangetast?
V = Vertrouwelijkheid	Hebben alleen rechthebbenden toegang tot de informatie/functie?

Welk niveau van beveiligingsmaatregelen geschikt is voor een bepaald informatiesysteem hangt af van de classificatie van de informatie die het systeem verwerkt.

Ten aanzien van beschikbaarheidseisen worden de volgende klassen onderscheiden:

Classificatie	**Definitie**
Niet vitaal	Algeheel verlies of niet beschikbaar zijn van deze informatie korter dan 1 week brengt geen schade toe aan de belangen van Nyenrode, haar medewerkers, haar studenten of klanten
Vitaal	Algeheel verlies of niet beschikbaar zijn van deze informatie voor maximaal 1 dag brengt geen schade toe aan de belangen van Nyenrode, haar medewerkers, haar studenten of klanten
Zeer vitaal	Algeheel verlies of niet beschikbaar zijn van deze informatie tot 1 uur brengt geen schade toe aan de belangen van Nyenrode, haar medewerkers, haar studenten of klanten

Voor zowel Vertrouwelijkheid als ook Integriteit wordt de volgende indeling gevolgd:

Classificatie	**Definitie**
Openbaar	• Iedereen mag de gegevens inzien, bijvoorbeeld de algemene website van Nyenrode • Een geselecteerde groep mag deze gegevens wijzigen
Intern	• Iedereen die aan Nyenrode is verbonden als medewerker, student of derde mag deze gegevens inzien; toegang kan zowel binnen als buiten Nyenrode (remote) worden verleend • Een geselecteerde groep mag deze gegevens wijzigen
Kritiek	• Er is expliciet aangegeven en geregistreerd wie welke rechten heeft t.a.v. de raadpleging en de verwerking van deze gegevens.

De classificatie dient door of namens de proces/systeem eigenaar van de betreffende informatie of van het betreffende informatiesysteem te worden bepaald.

Bijlage C Voorbeelden van datalekken

Voorbeelden van datalekken zijn:

- een kwijtgeraakte versleutelde USB-stick met persoonsgegevens;
- een verloren of gestolen versleutelde telefoon/laptop/tablet (privé of zakelijk) met persoonsgegevens of toegang tot een Nyenrode-account met persoonsgegevens;
- uitgeprinte documenten met persoonsgegevens die onbeheerd bij een kopieerapparaat liggen;
- anonieme enquêteresultaten die toch herleidbaar blijken te zijn tot respondenten;
- toegang tot persoonsgegevens die herleidbaar zijn tot natuurlijke personen waar je geen toegang toe zou moeten hebben;
- inbraak in een computer met persoonsgegevens of toegang tot een Nyenrode-account met persoonsgegevens door een hacker;
- rondsturen van een overzicht met namen, studentnummers en/of studieresultaten van studenten;
- rondsturen van een overzicht met namen, telefoonnummers en woonadressen van medewerkers;
- onbevoegden die camerabeelden kunnen inzien.

Voorbeelden van andere privacy incidenten zijn:

- gegevensverzameling die niet is gemeld bij *de FG*;
- onveilige werkwijze die kan leiden tot datalekken;
- gegevensverzameling op grond van toestemming van betrokkene zonder dat die toestemming daadwerkelijk gevraagd of geregistreerd wordt;
- het versturen van gevoelige (persoons)gegevens langs een onveilige weg of naar een onjuist e-mailadres (dus naar iemand waarnaar het niet bedoeld was);
- of inbraak in een computer met persoonsgegevens of toegang tot een Nyenrode account met persoonsgegevens door een hacker.