Developer Guidelines

Versie 26 januari 2023

1. Ontwikkelen in overeenstemming met de AVG

Of je alleen werkt, deel uitmaakt van een team dat een project ontwikkelt, een ontwikkelingsteam beheert of een serviceprovider bent die ontwikkelingen voor derden uitvoert, het is essentieel om ervoor te zorgen dat gebruikersgegevens en alle verwerking van persoonlijke gegevens gedurende de hele levenscyclus van het project voldoende worden beschermd.

De volgende stappen helpen bij het ontwikkelen van privacyvriendelijke applicaties of websites:

1.1. **Wees je bewust van de AVG-kernprincipes**

Binnen de subteams is de lead developer verantwoordelijk voor het toezicht op de naleving. Samen met de functionaris voor gegevensbescherming borgen we het begrijpen en voldoen aan de AVG-verplichtingen.

1.2. **Breng de gegevens en verwerking in kaart en categoriseer ze**

Door de gegevensverwerking die door een programma of toepassing wordt uitgevoerd nauwkeurig in kaart te brengen, kun je ervoor zorgen dat ze voldoen aan de wettelijke vereisten. Het bijhouden van een register van verwerkingsactiviteiten (voorbeeld), stelt ons in staat om een algemeen beeld van deze gegevens te hebben en om de bijbehorende risico's te identificeren en te prioriteren. Persoonlijke gegevens kunnen inderdaad op onverwachte plaatsen aanwezig zijn, zoals in serverlogboeken, cachebestanden, Excel-bestanden, enz., En kunnen op een aantal verschillende plaatsen worden opgeslagen.

1.3. **Prioriteer de vereiste acties**

Identificeer op basis van het gegevensverwerkingsregister de vereiste acties om te voldoen aan de verplichtingen van de AVG voorafgaand aan de ontwikkeling en prioriteer de aandachtspunten met betrekking tot de risico's voor de betrokkenen door de verwerking. Deze aandachtspunten hebben met name betrekking op de noodzaak en de soorten gegevens (zie hoofdstuk 8) die door onze software worden verzameld en verwerkt, de wettelijke basis waarop de gegevensverwerkingsactiviteiten zijn gebaseerd, de informatievermeldingen (zie hoofdstuk 13) van de software of applicatie, de contractuele clausules die we binden aan onze contractanten, de voorwaarden voor het uitoefenen van rechten, de maatregelen die zijn geïmplementeerd om onze verwerking te beveiligen.

1.4. **Beheer de risico's**

Wanneer we vaststellen dat een verwerking van persoonsgegevens waarschijnlijk hoge risico's voor betrokkenen met zich meebrengt, zorgen we er voor dat we die risico's op de juiste manier beheren in de context. Een Privacy Impact Assessment (PIA) kan helpen

die risico's te beheersen.

1.5. Interne processen opzetten

Om naleving tijdens alle ontwikkelingsfasen te garanderen, zorgen we ervoor dat interne procedures garanderen dat rekening wordt gehouden met gegevensbescherming in alle aspecten van het project en in alle gebeurtenissen die zich kunnen voordoen (bijv. inbreuk op de beveiliging, verzoeken om rectificatie of toegang tot uitvoering, wijziging van verzamelde gegevens, verandering van provider, gegevensinbreuk, enz.).

1.6. Naleving van documentontwikkelingen

Om te allen tijde aan te tonen dat we aan de AVG voldoen: de uitgevoerde acties en de documenten die in elke fase van de ontwikkeling worden geproduceerd, moeten onder de knie zijn. Dit impliceert in het bijzonder een regelmatige beoordeling en update van de documentatie van onze ontwikkelingen, zodat deze voortdurend consistent is met de functies die op ons programma zijn geïmplementeerd.

2. Identificeer persoonsgegevens

Het begrijpen van de begrippen "persoonlijke gegevens", "doel" en "verwerking" is essentieel voor de ontwikkeling van wetshandhavings- en gebruikersgegevens. Zorg er in het bijzonder voor dat je "anonimisering" en "pseudonimisering", die zeer nauwkeurige definities hebben in de AVG, niet verwart.

2.1. Definitie

- Het begrip **persoonsgegevens** wordt in de Algemene Verordening Gegevensbescherming (AVG) gedefinieerd als "alle informatie met betrekking tot een geïdentificeerde of identificeerbare natuurlijke persoon (aangeduid als "betrokkene")". Het bestrijkt een breed toepassingsgebied dat zowel direct identificeerbare gegevens (bijv. voor- en achternaam) als indirect identificerende gegevens omvat (bijv. telefoonnummer, kenteken, terminalidentificatie, enz.).

- Elke bewerking van dit soort gegevens (verzameling, registratie, overdracht, wijziging, verspreiding, enz.) vormt **een verwerking in de zin van de AVG** en moet daarom voldoen aan de vereisten van die verordening. Dergelijke verwerkingen moeten rechtmatig zijn en een bepaald doel hebben. De verzamelde en verwerkte persoonsgegevens moeten relevant zijn en beperkt tot wat strikt noodzakelijk is om het doel te bereiken.

2.2. Voorbeelden van persoonsgegevens

Wanneer zij betrekking hebben op natuurlijke personen, **zijn de volgende gegevens persoonsgegevens**:

- Naam, voornaam, pseudoniem, geboortedatum;
- foto's, geluidsopnamen van stemmen;

- vast of mobiel telefoonnummer, postadres, e-mailadres;
- IP-adres, computerverbindings-ID of cookie-ID;
- Vingerafdruk, handpalm of veneus netwerk van de hand, retinale afdruk;
- Kenteken, burgerservicenummer, ID-nummer;
- Gebruiksgegevens van applicaties, opmerkingen, enz...

Identificatie van natuurlijke personen kan worden uitgevoerd:

- uit één enkel stuk gegevens (voorbeelden: achternaam en voornaam);
- uit het kruisen van een reeks gegevens (bijvoorbeeld: een vrouw die op een dergelijk adres woont, geboren op die en die dag en lid van die en die vereniging).

Sommige gegevens worden als **bijzonder gevoelig** beschouwd. De AVG verbiedt het verzamelen of gebruiken van dergelijke gegevens, tenzij de betrokkene in het bijzonder zijn /haar uitdrukkelijke toestemming heeft gegeven (actieve, expliciete en bij voorkeur schriftelijke toestemming, die vrij, specifiek en geïnformeerd moet zijn).

Deze vereisten hebben betrekking op de volgende gegevens:

- gegevens met betrekking tot de **gezondheid van personen**;
- gegevens over **seksueel leven** of **seksuele geaardheid**;
- gegevens waaruit een vermeende **raciale** of **etnische** afkomst blijkt;
- politieke opvattingen, religieuze overtuigingen, filosofische overtuigingen of vakbondslidmaatschap;
- **genetische** en **biometrische gegevens die worden gebruikt om een persoon op unieke wijze te identificeren**.

2.3. Anonimisering van persoonsgegevens

Een **anonimiseringsproces van persoonsgegevens** heeft tot doel het identificeren van personen binnen datasets onmogelijk te maken. Het is dus een onomkeerbaar proces. Wanneer deze anonimisering effectief is, worden de gegevens niet langer beschouwd als persoonsgegevens en zijn de vereisten van de AVG niet langer van toepassing.

Standaard raden we aan **onbewerkte gegevenssets nooit als anoniem te beschouwen**. Anonimisering is het gevolg van de verwerking van persoonsgegevens om identificatie onomkeerbaar te voorkomen, hetzij door:

- *uitsplitsing* : het is niet mogelijk om sommige of alle records te isoleren die een individu in de dataset identificeren;
- *koppelbaarheid* : de dataset staat niet toe om ten minste twee records betreffende dezelfde betrokkene of een groep betrokkenen te koppelen;
- *gevolgtrekking* : het is niet mogelijk om, met significante waarschijnlijkheid, de waarde van een attribuut af te leiden uit de waarden van een reeks andere attributen.

Deze gegevensverwerkingsactiviteiten impliceren in de meeste gevallen een **kwaliteitsverlies op de geproduceerde dataset**. Het advies van de Groep artikel 29 (artikel 29 WP) over anonimiseringstechnieken beschrijft de belangrijkste anonimiseringstechnieken die vandaag de dag worden gebruikt, evenals voorbeelden van datasets die ten onrechte als anoniem

worden beschouwd. Het is belangrijk op te merken dat anonimiseringstechnieken tekortschieten. De keuze om de gegevens al dan niet te anonimiseren en de selectie van een anonimiseringstechniek moeten van geval tot geval worden gemaakt op basis van de context van gebruik en behoefte (aard van de gegevens, bruikbaarheid van de gegevens, risico's voor mensen, enz.).

2.4. Pseudonimisering van persoonsgegevens

Pseudonimisering is een compromis tussen het bewaren van ruwe gegevens en het produceren van geanonimiseerde datasets.

Het verwijst naar de verwerking van persoonsgegevens op een zodanige manier dat **gegevens met betrekking tot een natuurlijke persoon niet langer kunnen worden toegeschreven zonder aanvullende informatie**. De AVG staat erop dat deze aanvullende informatie afzonderlijk moet worden bewaard en onderworpen moet zijn aan technische en organisatorische maatregelen om te voorkomen dat betrokkenen opnieuw worden geïdentificeerd. In tegenstelling tot anonimisering kan pseudonimisering een omkeerbaar proces zijn.

In de praktijk bestaat een pseudonimiseringsproces uit **het vervangen van direct identificerende gegevens (achternaam, voornaam, enz.) in een dataset door indirect identificerende gegevens** (alias, nummer in een archiefsysteem, enz.) om hun gevoeligheid te verminderen. Ze kunnen het gevolg zijn van een cryptografische hash van de gegevens van individuen, zoals hun IP-adres, gebruikers-ID, e-mailadres.

Gegevens die voortvloeien uit pseudonimisering worden beschouwd als **persoonsgegevens en blijven daarom onderworpen aan de verplichtingen**. De Europese verordening moedigt echter het gebruik van pseudonimisering aan bij de verwerking van persoonsgegevens. Bovendien is de AVG van mening dat pseudonimisering het mogelijk maakt om de risico's voor betrokkenen te verminderen en bij te dragen aan de naleving van de verordening.

3. Bereid je ontwikkeling voor

De beginselen van de bescherming van persoonsgegevens moeten vanaf de ontwerpfase worden geïntegreerd in de IT-ontwikkelingen om de privacy te beschermen van de mensen van wie je de gegevens gaat verwerken, om hen een betere controle over hun gegevens te geven en om fouten, verliezen, ongeoorloofde wijzigingen of misbruik van hun gegevens in applicaties te beperken.

3.1. Methodologische keuzes

- **Zet privacybescherming centraal in uw ontwikkelingen** door een Privacy By Design-methodologie te gebruiken.
- Als je agile methoden gebruikt voor je ontwikkelingen, overweeg dan om beveiliging centraal in het proces te integreren. Security within agile environments geeft aan hoe je je ontwikkelingen kunt uitvoeren in het kader van een agile methode, rekening houdend met de beveiligingsaspecten. Maar ook Agile tools als Azure DevOps boards of Jira kunnen helpen om security op te nemen in elk work-item / product backlog item.

- Voor elke ontwikkeling gericht op het grote publiek, **moet rekening worden gehouden met de privacy-instellingen**, en in het bijzonder de standaardinstellingen, zoals de kenmerken en gebruikersinhoud die standaard zichtbaar zijn.
- Voer een Privacy Impact Assessment (PIA) uit. Voor bepaalde verwerkingen is het verplicht. In andere gevallen is het een goede praktijk waarmee je alle risico's voorafgaand aan je ontwikkelingen kunt identificeren en afhandelen.

4. Beveilig je ontwikkelomgeving

De beveiliging van productie-, ontwikkelings- en continue integratieservers en ontwikkelaarswerkstations moet een prioriteit zijn omdat ze de toegang tot een grote hoeveelheid gegevens centraliseren.

4.1. Beoordeel risico's en neem de juiste beveiligingsmaatregelen

- **Beoordeel de risico's** in de tools en processen die worden gebruikt voor je ontwikkelingen. Inventariseer bestaande beveiligingsmaatregelen en stel een actieplan op om risicodekking te verbeteren. Benoem een persoon die verantwoordelijk is voor de uitvoering ervan.
- Overweeg de risico's op alle tools die je gebruikt, inclusief risico's met betrekking tot SaaS (Software as a Service) en samenwerkingstools in de cloud (zoals Slack, Trello, GitHub, enz.).

4.2. Beveilig servers en werkstations op een homogene en reproduceerbare manier

- Lijsten met **aanbevelingen** met betrekking tot de beveiliging van servers, werkstations en interne netwerken zijn beschikbaar in hoofdstukken 6 tot en met 9.
- Schrijf een document met deze maatregelen en leg hun configuratie uit om ervoor te zorgen dat beveiligingsmaatregelen uniform worden geïmplementeerd op servers en werkstations. Om de werklast te verminderen, kunnen configuratiebeheertools, zoals Ansible, Puppet of Chef, worden gebruikt.
- Update servers en werkstations, indien mogelijk automatisch. Je kunt een watchlist instellen van de belangrijkste kwetsbaarheden, bijvoorbeeld de NVD Data Feeds.

4.3. Bijzondere nadruk leggen op toegangsbeheer en traceerbaarheid van activiteiten

- Vergeet niet om het beheer van SSH-sleutels te documenteren (gebruik van state-of-the-art cryptografie en sleutellengte-algoritmen, bescherming van privésleutels met een wachtwoordzin, sleutelrotatie). Voor voorbeelden van goede praktijken, zie de website van (open)SSH.
- Stimuleer sterke authenticatie op de services die door het ontwikkelingsteam worden gebruikt.
- Traceer de toegang tot machines en implementeer, indien mogelijk, geautomatiseerde loganalyse. Om betrouwbare sporen te behouden, moet het gebruik van generieke accounts worden vermeden.

5. Beheer je broncode

Ongeacht de grootte van je project, wordt het ten zeerste aanbevolen om een

broncodebeheertool te gebruiken, zoals een versiebeheersysteem, om de verschillende versies in de loop van de tijd bij te houden.

5.1. Stel je versiebeheersysteem efficient in, nadenkend over de beveiliging ervan

- Een versiebeheersysteem is een softwareprogramma waarmee je **al je broncode en bijbehorende bestanden** kunt opslaan, terwijl je de **chronologie van alle aangebrachte wijzigingen** behoudt. Een eenvoudige FTP-server is geen versiebeheersysteem.
- Stel je omgeving correct in met behulp van de functies van je versiebeheersysteem. Het wordt aanbevolen om aan het begin van je project sterke **verificatie** en/of **verificatie met SSH-sleutels** te implementeren.
- Wijs bovendien toegangsniveaus tot je project toe aan de gebruikers van je versiebeheersysteem en definieer voor elk niveau de bijbehorende **machtigingen** (bijvoorbeeld een "gast" -niveau met beperkte leesrechten, een "ontwikkelaar" -niveau met schrijfrechten, enz.).
- Maak regelmatig **back-ups** van je broncodebeheersysteem. Vergeet in het bijzonder niet om een back-up te maken van je hoofdserver waar alle wijzigingen worden opgeslagen.
- Stel ontwikkelingsprocedures in om efficiënt te werken, zelfs als **meerdere mensen tegelijkertijd ontwikkelen**. Je kunt bijvoorbeeld besluiten om niet aan dezelfde vertakking (master) te werken, maar om op functies gebaseerde vertakkingen in te stellen, die naarmate de ontwikkeling vordert, worden samengevoegd met de hoofdtak. Dergelijke ontwikkelingsstrategieën zijn al goed gedocumenteerd, bijvoorbeeld in de trunk-based workflow of Git Flow. Bovendien bieden sommige versiebeheersystemen aan om **beveiligde vertakkingen** in te stellen die ongeoorloofde wijzigingen in de bestanden in deze vertakkingen voorkomen.

5.2. Wees je bewust van de inhoud van je broncode

- Implementeer tools voor codekwaliteitsstatistieken die je code scannen zodra deze is toegezegd om de goede kwaliteit ervan te controleren. Je kunt ook scripts toevoegen om deze statistieken te controleren in de configuratie van het versiebeheersysteem: de commit wordt geannuleerd als de broncode niet van voldoende kwaliteit is.
- Houd geheimen en wachtwoorden uit de broncoderepository:
    - in afzonderlijke **dossiers, die niet zijn vastgelegd**. Vergeet niet om speciale bestanden van je versiebeheersysteem te gebruiken (zoals .gitignore voor Git), zodat u niet per ongeluk gevoelige bestanden vastlegt.
    - in **omgevingsvariabelen**, zorg ervoor dat je controleert of omgevingsvariabelen niet per ongeluk naar logboeken worden geschreven of worden weergegeven wanneer een toepassingsfout optreedt.
    - met behulp van specifieke geheime of configuratiebeheersoftware.

Ten slotte, als je dergelijke gegevens in je repository moet opnemen, overweeg dan om de bestanden automatisch te versleutelen / decoderen met behulp van een plug-in van je versiebeheersysteem (bijv. git-crypt).

- Vergeet na een commit die persoonlijke of andere kritieke gegevens bevat, niet om de broncoderepository volledig te verwijderen: zelfs na wijziging kunnen de gegevens nog steeds beschikbaar zijn in je repositorygeschiedenis.

- Wees voorzichtig voordat je je broncode online publiceert. Controleer de volledige inhoud om er zeker van te zijn dat er geen persoonlijke gegevens, wachtwoorden of andere geheimen aanwezig zijn, inclusief de volledige wijzigingsgeschiedenis.

5.3. Voorbeelden van tools

- In tegenstelling tot tools zoals Subversion, die een centrale server nodig hebben om te draaien, zijn de belangrijkste versiebeheersystemen (Git, Mercurial bijvoorbeeld) gedecentraliseerd.
- Voor de meeste van deze tools zijn een webinterface en gerelateerde tools (bugbeheer, wiki voor je documentatie, enz.) beschikbaar. Deze oplossingen kunnen toegankelijk zijn via het internet (GitHub, Bitbucket, etc.), of ze kunnen worden geïntegreerd in je eigen servers.

5.4. Lokale PC/Laptop

- Aangezien broncode ook bij meerdere ontwikkelaars op de lokale PC/laptop komt te staan is er **een risico dat een kwaadwillende** op die manier aan de broncode kan komen (bijv. bij diefstal van een laptop). Broncode is een belangrijke bron voor het zoeken naar kwetsbaarheden in de software, **dus ook lokale omgevingen dienen veilig te zijn** (goede wachtwoorden, Bitlocker e.d.).

6. Maak een weloverwogen architectuurkeuze

Bij het ontwerpen van de architectuur van je toepassing moet je persoonlijke gegevens identificeren die worden verzameld en een pad en levenscyclus voor elk van hen definiëren. De keuze van ondersteunende assets (lokale opslag, server, cloudservice) is een cruciale stap, die moet worden aangepast aan je behoeften, maar ook aan je technische kennis. Het register en de uitvoering van een privacy impact beoordeling kan je helpen bij deze keuze.

6.1. Onderzoek naar de levenscyclus van gegevens en processen, van verzameling tot verwijdering

- Vertegenwoordig en beschrijf hoe het product in het algemeen werkt voordat je aan je project begint, met een diagram van gegevensstromen en een gedetailleerde beschrijving van de uitgevoerde processen.

- Wanneer gegevens alleen **worden opgeslagen op de terminal van de gebruiker** (lokale opslag) of beperkt blijven **tot communicatienetwerken onder controle van de gebruiker** (bijv. Wi-Fi of een ander lokaal netwerk), is het belangrijkste aandachtspunt de gegevensbeveiliging. De duur waarvoor gegevens worden opgeslagen en de daadwerkelijke verwijdering moeten door de personen worden bepaald.

- **Wanneer de gegevens via online diensten worden verzonden**, moet de keuze om de gegevens zelf te hosten of een serviceprovider te gebruiken, worden gemaakt op

basis van je beveiligingskennis en de verwachte kwaliteit van de dienstverlening. Erkende cloudaanbiedingen kunnen hogere beveiligingsniveaus bieden. Ze genereren echter nieuwe risico's die moeten worden beheerst.

6.2. In geval van gebruik van externe hosting

- **Kies een dienstverlener die zorgt voor passende beveiligings- en vertrouwelijkheidsmaatregelen en voldoende transparant is.**

- **Zorg ervoor dat je de geografische locatie kent van de servers die je gegevens hosten**. Mogelijk moet je gegevens overdragen buiten de Europese Unie (EU) en de Europese Economische Ruimte (EER). Hoewel gegevens vrij kunnen circuleren binnen de EU/EER, zijn overdrachten buiten de EU/EER mogelijk, op voorwaarde dat een voldoende en passend niveau van gegevensbescherming wordt gewaarborgd. De CNIL biedt een on-site kaart met de verschillende niveaus van gegevensbescherming in landen over de hele wereld.

- **Als je medische gegevens moet hosten**, moet je ervoor zorgen dat de gebruikte provider is gecertificeerd of goedgekeurd voor deze activiteit.

- Andere punten om rekening mee te houden zijn:
    - het bestaan van een toegankelijk beveiligingsbeleid;
    - fysieke beveiligings- en veiligheidsmaatregelen op de hostingsite;
    - gegevensversleuteling en andere processen om ervoor te zorgen dat de aanbieder geen toegang heeft tot de aan hem toevertrouwde gegevens;
    - het beheer van updates, het beheer van autorisaties, de authenticatie van personeel en de beveiliging van applicatieontwikkelingen;
    - de eenvoudige omkeerbaarheid/overdraagbaarheid van gegevens in een gestructureerd en algemeen gebruikt formaat, op verzoek en op elk moment.

7. Beveilig je websites, applicaties en servers

Elke website, applicatie of server moet elementaire state-of-the-art beveiligingsregels bevatten, niet alleen voor netwerkcommunicatie, maar ook voor authenticatie en infrastructuur.

7.1. Communicatienetwerken beveiligen

- **Implementeer TLS versie 1.2 of 1.3** (ter vervanging van SSL) op alle websites en voor gegevensoverdrachten van je mobiele applicaties, bijvoorbeeld met LetsEncrypt, waarbij alleen de meest recente versies worden gebruikt en de juiste implementatie wordt gecontroleerd.

- **Maak het gebruik van TLS verplicht** voor alle pagina's van je site en voor je mobiele applicaties.

- **Beperk de communicatiepoorten** die strikt noodzakelijk zijn voor de goede werking van de geïnstalleerde toepassingen. Als toegang tot een webserver alleen mogelijk is

via het HTTPS-protocol, moeten alleen poort 443 en 80 van deze server toegankelijk zijn, alle andere poorten kunnen door de firewall worden geblokkeerd.

- **De OWASP heeft op haar website enkele cheatsheets gepubliceerd** om TLS correct te implementeren of een webservice te beveiligen.

7.2. Verificaties beveiligen

- **Volg** de Microsoft-aanbeveling over wachtwoorden. Vergeet in het bijzonder niet om het aantal toegangspogingen te beperken.

- **Sla wachtwoorden** nooit **op in leesbare tekst**. Sla ze op als een hash met behulp van een bewezen bibliotheek, zoals bcrypt.

- **Als cookies worden gebruikt voor authenticatie**, wordt het aanbevolen:
  - om het gebruik van HTTPS via HSTS af te dwingen;
  - om de beveiligde vlag te gebruiken;
  - gebruik de httponly-vlag.

- **Test de cryptografische suites** die **op de systemen zijn geïnstalleerd** en schakel verouderde suites uit (RC4, MD4, MD5 enz.). Stimuleer het gebruik van AES256. Lees de OSWAP-notitie over dit onderwerp.

- **Hanteer een specifiek wachtwoordbeleid voor beheerders**. Wijzig de wachtwoorden ten minste elke keer dat een beheerder vertrekt en in geval van vermoedelijke inbreuk. Moedig waar mogelijk sterke authenticatie aan.

- **Beperk de toegang tot beheertools en interfaces tot gekwalificeerd personeel**. Stimuleer het gebruik van accounts met lagere bevoegdheden voor dagelijkse activiteiten.

- Voor toegang op afstand **tot beheerinterfaces moeten verhoogde beveiligingsmaatregelen gelden**. Voor interne servers kan het implementeren van een VPN met sterke authenticatie van de gebruiker en het werkstation dat hij of zij gebruikt bijvoorbeeld een goede oplossing zijn.

7.3. Infrastructuur beveiligen

- **Maak back-ups, indien mogelijk versleuteld en regelmatig gecontroleerd**. Dit is vooral handig in het geval van een ransomware-aanval op je systemen, omdat het hebben van back-ups voor al je systemen de enige maatregel is waarmee je je systemen kunt herstellen.

- **Beperk de grootte van de gebruikte softwarestack** en voor elk element van de stack:
  - **Installeer kritieke updates** zonder vertraging door een automatische wekelijkse controle te plannen;

    - **Automatiseer een vulnerability watch** door je bijvoorbeeld te abonneren op de NVD Data Feeds.

- **Gebruik hulpprogramma's** voor **het detecteren van** kwetsbaarheden voor de meest kritieke processen om mogelijke inbreuken op de beveiliging te detecteren. Systemen voor het detecteren en voorkomen van aanvallen op kritieke systemen of servers kunnen ook worden gebruikt. Deze tests moeten regelmatig worden uitgevoerd en voordat een nieuwe softwareversie in productie wordt genomen.

- **Beperk of verbied fysieke en softwaretoegang tot diagnostische en externe configuratiepoorten**. Je kunt bijvoorbeeld alle geopende poorten weergeven met behulp van de netstat-tool.

- **Bescherm de databases die je op internet beschikbaar stelt**, ten minste door de toegang zoveel mogelijk te beperken (bijvoorbeeld door IP-filtering) en door het standaardwachtwoord voor de beheerdersaccount.

- Op het gebied van databasebeheer omvatten goede praktijken:
    - **het gebruik van nominatieve accounts** voor databasetoegang en het maken van specifieke accounts voor elke toepassing;
    - **het intrekken van de beheerdersrechten** van gebruikers- of toepassingsaccounts om wijzigingen in de databasestructuur (tabel, vues, proces, enz.) te voorkomen;
    - bescherming hebben tegen SQL- of scriptinjectie-aanvallen;
    - het aanmoedigen van schijf- en databaseversleuteling in rust.

8. Minimaliseer de gegevensverzameling

Je zal alleen persoonsgegevens verzamelen die adequaat, relevant en noodzakelijk zijn in verband met de doeleinden waarvoor ze worden verwerkt, zoals gedefinieerd op het moment van verzamelen.

8.1. Denk voor het verzamelen na over de verschillende soorten gegevens die je moet verzamelen en probeer je verzameling te beperken tot wat strikt noodzakelijk is

- Denk na over de verschillende **soorten gegevens** die moeten worden verzameld voordat een toepassing wordt geïmplementeerd en documenteer dit denken.

- Als specifieke gegevens niet **nodig zijn voor een bepaalde categorie mensen**, verzamel deze dan niet.

- Verwerk en bewaar gegevens op een manier die **de nauwkeurigheid vermindert** (vergelijkbaar met pseudonimisering). Bewaar bijvoorbeeld alleen het geboortejaar in plaats van een volledige geboortedatum als de aanvraag alleen het jaar nodig heeft.

- Als je bijzonder gevoelige gegevens verzamelt, zoals gegevens over gezondheid of strafrechtelijke veroordelingen, zorg er dan voor dat je alleen het **minimaal vereiste verzamelt**. Vanwege de wettelijke beperkingen is de eenvoudigste oplossing nog steeds om **ze niet te verzamelen** als je zonder hen kunt.

- Minimaliseer de hoeveelheid verzamelde gegevens ook in de **loggegevens** en sla geen gevoelige of kritieke gegevens op (gezondheidsgegevens, wachtwoorden, enz.). Meestal zijn gevoelige gegevens helemaal niet nodig in logging, dus ook geen namen of studentnummers. Beperk ook de toegang tot loggegevens, zodat bijv. niet iedere ontwikkelaar productie-loggegegevens kan inzien.

- Sommige functies kunnen de gebruikerservaring verbeteren, maar zijn **niet strikt noodzakelijk om je toepassing goed te laten werken** (bijv. geolocatie om een geografische zoekopdracht te vereenvoudigen). In dit geval moet de eindgebruiker kunnen **kiezen of hij deze functionaliteit al dan niet gebruikt**. Als hij het gebruikt, mogen de gegevens die je voor de werking ervan moet verzamelen, alleen worden bewaard voor de tijd die strikt noodzakelijk is voor de werking ervan en nooit voor andere doeleinden worden gebruikt.

- Vergeet niet om **bewaartermijnen** te koppelen voor elke categorie gegevens, afhankelijk van het doel van de verwerking en de wettelijke of reglementaire verplichtingen met betrekking tot het bewaren ervan. Logboeken moeten ook een bewaartermijn hebben. Documenteer de gedefinieerde bewaarduur. Je zult ze moeten kunnen rechtvaardigen.

8.2. Zodra de gegevens zijn verzameld, stel je automatische verwijderingsmechanismen in

- Implementeer een automatisch spoelsysteem aan het einde van de houdbaarheid. Je kan ook handmatige beoordelingen van opgeslagen gegevens op periodieke basis implementeren.

- Om volledige verwijdering te garanderen, wis **je fysiek** alle gegevens die niet langer nodig zijn met behulp van gespecialiseerde hulpmiddelen of door de fysieke media te vernietigen.

- Als de gegevens nog steeds nuttig zijn, kun je de gevoeligheid ervan verminderen door **pseudomisatie-** of zelfs **anonimiseringsmethoden** te gebruiken. In geval van pseudonimisering blijven deze gegevens onderworpen aan de regelgeving inzake persoonsgegevens (zie hoofdstuk 2).

- Log de **automatische verwijderingsprocedures**. De bijbehorende logboeken kunnen worden gebruikt als **bewijs van verwijdering** van een gegevensitem.

9. Gebruikersprofielen beheren

De manier om profielen van je medewerkers en je eindgebruikers te beheren, moet voorafgaand aan je ontwikkelingen worden doordacht. Het bestaat uit het definiëren van verschillende toegangs- en autorisatieprofielen, zodat elke persoon alleen toegang heeft tot de gegevens die hij of zij daadwerkelijk nodig heeft.

9.1. Goede praktijken voor gebruikersbeheer

- Het begint allemaal met het **gebruik van unieke en individuele id's**, of het nu gebruikers van uw toepassing zijn of bijdragers in ontwikkeling.

- Zorg ervoor dat **je authenticatie oplegt** voordat je toegang krijgt tot persoonlijke gegevens, in overeenstemming met de aanbevelingen van het gebruik van sterke wachtwoorden.

- Om ervoor te zorgen dat elke persoon (gebruiker of medewerker) alleen toegang heeft tot **gegevens die hij of zij daadwerkelijk nodig heeft**, moet je systeem **gedifferentieerd beleid voor gegevenstoegangsbeheer** bieden (lezen, schrijven, verwijderen, enz.) op basis van mensen en behoeften. Met een algemeen mechanisme voor gebruikersprofielbeheer kunt je verschillende rechten groeperen op basis van een rol die wordt uitgeoefend door een groep gebruikers binnen de toepassing.

- Het beheer van gebruikersprofielen kan samen met **logsystemen worden gebruikt om activiteiten te traceren en anomalieën of gebeurtenissen met betrekking tot beveiliging te detecteren**, zoals frauduleuze toegang en misbruik van persoonlijke gegevens. Deze apparaten mogen niet voor andere doeleinden worden gebruikt dan het waarborgen van het juiste gebruik van het computersysteem. Logboeken mogen ook niet langer worden bewaard dan nodig is. Over het algemeen is een periode van zes maanden voldoende.

- Je kunt ook code-audits of penetratietests plannen binnen je ontwikkelomgeving om **de robuustheid van je profielbeheersysteem te garanderen**.

9.2. Stroomlijn het beheer van opruimingsprofielen

- Plan om **de bewegingen van je medewerkers te documenteren of te automatiseren**. Deze procedures moeten bijvoorbeeld leiden tot de acties die moeten worden ondernomen wanneer mensen niet langer gemachtigd zijn om toegang te krijgen tot een ruimte of een IT-bron, of aan het einde van hun contract.

- Het beheren van je gebruikers en medewerkers impliceert **een regelmatige herziening van de toestemming** op basis van de evolutie van het gebruik en de organisatorische bewegingen binnen je project. Het gebruik van directoryservices, zoals LDAP (Lightweight Directory Access Protocol), helpt je deze wijzigingen te controleren en stelt je in staat je toegangsstrategieën te verfijnen, bijvoorbeeld door

rollen toe te wijzen op basis van gebruiksprofielen. Hierdoor kan je het principe van het minste privilege beter respecteren.

- Het gebruik van "supreme" accounts (type root, administrator, enz.) moet worden vermeden voor conventionele bewerkingen, omdat het de hoeksteen van je systeem vormt en een geprivilegieerd doelwit voor een mogelijke externe aanvaller. We raden je aan er een sterk wachtwoordbeleid aan te koppelen (10 tot 20 tekens of multifactor) en het aantal mensen met kennis ervan te beperken tot het striktste noodzakelijke.

- **Geef de voorkeur aan het gebruik van een wachtwoordmanager binnen je project** en de overgang naar sterke authenticatie waar mogelijk. Vermijd generieke accounts die door meerdere mensen worden gedeeld.

10. Beheer je bibliotheken en SDK's

Gebruik je bibliotheken, SDK's of andere softwarecomponenten die door derden zijn geschreven? Hier zijn een paar tips over hoe je deze tools kunt integreren terwijl je de controle houdt over je ontwikkelingen.

Let op: Wordt de ontwikkelde software na ontwikkeling als open source aangeboden? Ga dan na of de softwarecomponenten van die derden ook als open source aangeboden worden en of je uberhaupt het (intellectueel eigendoms- of auteurs-) recht hebt om deze componenten te gebruiken.

10.1. Maak een weloverwogen keuze

- **Beoordeel de waarde van het toevoegen van elke afhankelijkheid**. Sommige veelgebruikte softwarestenen zijn slechts een paar regels lang. Elk toegevoegd element is echter een toename van het aanvalsoppervlak van je systeem. In het geval dat een enkele bibliotheek meerdere functionaliteiten biedt, integreer dan alleen de functionaliteiten die je daadwerkelijk nodig hebt. Door het minimale aantal functionaliteiten te activeren, verminder je het aantal potentiële bugs dat kan optreden.

- **Kies onderhouden software, bibliotheken en SDK's**:
    - Als je gratis of open source software wilt gebruiken, probeer dan projecten of oplossingen te kiezen met een actieve community, regelmatige updates en goede documentatie. Als je open source gebruikt, kijk dan goed of de betreffende licentie het toe staat dat de open source component in een later stadium juist niet open source gebruikt wordt.
    - Als je andere soorten oplossingen met commerciële ondersteuning gebruikt, zorg er dan contractueel voor dat de code gedurende de levensduur van je project wordt onderhouden en bijgewerkt. Wordt de ontwikkelde software na ontwikkeling als open source aangeboden? Ga dan vooraf na of de softwarecomponenten van die derden ook als open source aangeboden

mogen worden.

- **Houd rekening met privacy**. Sommige SDK's of bibliotheken betalen zichzelf terug door persoonlijke gegevens te gebruiken die zijn verzameld via de applicaties of sites waarop ze zijn geïntegreerd. Zorg ervoor dat dergelijke derden voldoen aan de toepasselijke wetgeving met betrekking tot persoonsgegevens, inclusief een mechanisme voor het verkrijgen van toestemming van de gebruiker.

- **Als je cryptografische mechanismen gebruikt, wordt het sterk afgeraden om zelf cryptografische algoritmen of protocollen te implementeren**, maar probeer cryptografische bibliotheken te kiezen die worden onderhouden, herkend en gemakkelijk te gebruiken.

- Houd rekening met **intellectueel eigendom en auteursrechten**. Bij ontwikkelen van software heb je te maken met intellectueel eigendom van de auteursrechthebbende. Dat ben je zelf of wanneer je in dienstverband iets ontwikkelt, je werkgever. Meer informatie over IE: Checklist Intellectueel Eigendom Labs

10.2. Evalueer de geselecteerde elementen

- **Lees de documentatie en wijzig de standaardconfiguraties**. Het is belangrijk om te weten hoe je afhankelijkheden werken. Bibliotheken en SDK's van derden worden vaak geleverd met standaardconfiguratiebestanden, die zelden worden gewijzigd vanwege tijdgebrek, wat veel beveiligingslekken veroorzaakt.

- **Controleer je bibliotheken en SDK's**. Weet je echt wat alle bibliotheken en SDK's die je integreert doen? Welke gegevens worden via deze afhankelijkheden verzonden en naar wie? Met deze audit kan je bepalen welke verplichtingen inzake gegevensbescherming moeten worden nageleefd en de verantwoordelijkheid van de actoren vaststellen.

- **Breng je afhankelijkheden in kaart**. Bibliotheken en SDK's van derden kunnen ook andere componenten integreren: door hun code te controleren, kan je al je afhankelijkheden beter in kaart brengen en beter handelen als een probleem een van hen treft. Het wordt ook aanbevolen dat je beveiligingsaudits van je onderdelen van derden uitvoert en deze controleert.

- **Pas op voor typosquatting en andere kwaadaardige technieken**. Controleer de namen van afhankelijkheden, evenals hun eigen afhankelijkheden om aanvallen te voorkomen. Kopieer en plak geen opdrachtregels van onbekende sites.

10.3. Bibliotheken en SDK's onderhouden

- **Gebruik afhankelijkheidsbeheersystemen** (zoals yum, apt, maven, pip, enz.) om een up-to-date lijst van je afhankelijkheden bij te houden.

- **Beheer updates voor je afhankelijkheden**, vooral in het geval van beveiligingsupdates die kwetsbaarheden verhelpen. Je moet een gedocumenteerde procedure instellen om deze zo snel mogelijk te beheren en te implementeren.

- **Houd rekening met de versies van bibliotheken en SDK's aan het einde van de ondersteuning** die niet langer worden onderhouden: probeer een andere oplossing te vinden (kies een nieuwe bibliotheek, verleng commerciële ondersteuning).

- **Controleer de status van open-sourceprojecten**, met name de verandering van domein- of pakketeigendom, sommige aanvallen met behulp van kwaadaardige updates van populaire afhankelijkheden.

- **Pas tooling in de (build) pipeline toe** die scannen op bekende kwetsbaarheden in gebruikte bibliotheken.

11. Zorg voor de kwaliteit van de code en de bijbehorende documentatie

Het is essentieel om zo snel mogelijk goede technieken voor het schrijven van code toe te passen. Leesbaarheid van code vermindert de inspanning van onderhoud en bugfixes in de loop van de tijd voor jezelf en je (mogelijk toekomstige) collega's.

11.1. Documentcode en architectuur

- Documentatie wordt soms weggelaten tijdens de ontwikkeling, vanwege gebrek aan tijd of zichtbaarheid op het project. Het is echter **cruciaal voor de onderhoudbaarheid van je project**: het stelt je in staat om te begrijpen hoe de code wereldwijd werkt en om te weten welke delen van de code worden beïnvloed door een wijziging. Als SOLID-pricinciples zo goed mogelijk worden gevolgd, kan documentatie van code een stuk eenvoudiger zijn, aangezien de code zelf al veel beter leesbaar / begrijpbaar is.

- **Documenteer de architectuur, niet alleen de code**: je moet het grote geheel in gedachten kunnen houden wanneer je je documentatie schrijft en ontwikkelaars helpen begrijpen hoe al je componenten samenwerken. Richt je daarom op diagrammen en duidelijke uitleg bij het documenteren van je project.

- **Onderhoud de documentatie samen met de code:** De beste manier om je documentatie up-to-date te houden, is door deze te wijzigen terwijl je met de code meegaat. Echter, door code niet onnodig uitgebreid te documenteren, is deze taak een stuk eenvoudiger. Goed geschreven code heeft minimale documentatie nodig en dat is dan in de praktijk ook veel beter te onderhouden.

- Als je een broncodebeheerder gebruikt, kan je ook documentatiewijzigingen opnemen voor elke "commit" die je code wijzigt (zie met name Hoofdstuk 5).

- **Vergeet niet om beveiliging in je documentatie aan te pakken**. Je kan met name de verschillende configuratiekeuzes voor je toepassing documenteren en uitleggen welke instellingen het veiligst zijn.

11.2. Controleer de kwaliteit van je code en de bijbehorende documentatie

- Een kwaliteitscode omvat **de goedkeuring van goede praktijken en coderingsconventies** die consistent worden toegepast in het hele programma. Het is ook het beste om te verwijzen naar bestaande conventies. Hier zijn een paar voorbeelden van goede praktijken:
    - **Het gebruik van expliciete variabele- en functienamen** maakt het gemakkelijker om op het eerste gezicht te begrijpen wat er aan de hand is.
    - **Door uw code correct** in te laten springen, kunt u de structuur van de code sneller zien.
    - **Het vermijden van coderedundantie** vermindert de correctie-inspanningen die op verschillende plaatsen moeten worden uitgevoerd. Een vergissing wordt snel vergeten.

- **Tools kunnen u helpen de kwaliteit van uw code te controleren**. Eenmaal correct ingesteld, zullen ze voorkomen dat ze de code opnieuw lezen om de juiste implementatie van coderingsconventies te controleren. Voorbeelden van deze tools zijn:
    - **Geïntegreerde ontwikkelomgevingen** ("IDE"), mogelijk met behulp van plug-ins ("plug-ins"), kunnen worden geconfigureerd om code-indentatieregels, regeleinden tussen verschillende delen van code of de positie van accolades en andere haakjes te respecteren.
    - **Software voor het meten van de kwaliteit van de broncode** kan codeduplicaties, naleving van programmeerregels of potentiële bugs melden. Maar ook (bijvoorbeeld via SonarCube) controles opnemen in de build pipelines.

12. Test je toepassingen

Door je product te testen, kan je de juiste werking controleren, een goede gebruikerservaring garanderen en defecten vinden en voorkomen voordat het in productie gaat. Het testen van je product vermindert ook het risico op inbreuken op persoonsgegevens.

12.1. Testen automatiseren

- De **ontwikkelingstests** (eenheid, functioneel, enz.) zullen de geschiktheid tussen de specificaties en de werking van het product verifiëren. De **beveiligingstests** (willekeurige gegevenstests ook wel "fuzzing" genoemd, scan van kwetsbaarheden, enz.), Zullen controleren of het product acceptabel blijft functioneren wanneer je afstapt van het normale gebruik en dat het geen kwetsbaarheid vertoont waardoor derden de beveiliging in gevaar kunnen brengen. Beide soorten testen zijn belangrijk voor het goed functioneren van je applicatie.

- Stel een **continu integratiesysteem** in om de tests automatisch uit te voeren na elke wijziging in je broncode.

12.2. Integreer testen in je bedrijfsstrategie

- Voeg de implementatie van de testomgeving toe aan de strategie van het bedrijf. De **aanvaardbare statistieken** moeten voorafgaand aan de ontwikkeling gezamenlijk door alle partijen worden gedefinieerd.

- Statistieken om te overwegen zijn bijvoorbeeld:
    - De **dekkingsgraad** van tests en hun type;
    - de **duplicatiesnelheid** van je code;
    - het **aantal kwetsbaarheden** (zoals gedefinieerd door de tools) en hun type, enz.

12.3. Let op je testgegevens!

- "Echte" productiegegevens mogen niet worden gebruikt tijdens de ontwikkelings- en testfase. Het gebruik van persoonsgegevens uit je productiedatabase voor testdoeleinden komt neer op **het afleiden van persoonsgegevens uit je productiedatabase van het oorspronkelijke doel**.

- Als persoonsgegevens buiten productie worden gebruikt, moet worden opgemerkt dat de **beveiligingsrisico's** ook worden **verhoogd**: toegang tot de gegevens door mensen die het niet nodig hebben om te weten, meerdere opslaglocaties, enz.

- Bouw dus een **dummy-dataset** die eruitziet als de gegevens die door je toepassing worden verwerkt. Een dummy dataset zorgt ervoor dat openbaarmaking van deze gegevens geen impact heeft op mensen.

- Als je **bestaande configuraties** uit productie in je testcases moet importeren, kan je overwegen **de persoonlijke gegevens** die aanwezig kunnen zijn te anonimiseren.

13. Informeer gebruikers

Het transparantiebeginsel van de AVG vereist dat alle informatie of communicatie met betrekking tot de verwerking van persoonsgegevens beknopt, transparant, begrijpelijk en gemakkelijk toegankelijk is in duidelijke en eenvoudige taal.

13.1. Wie te informeren en wanneer?

- De betrokkenen moeten worden geïnformeerd:
    - zowel **in het geval van directe gegevensverzameling**, d.w.z. wanneer gegevens rechtstreeks van individuen worden verzameld (voorbeelden: vorm, online aankoop, abonnement op een contract, opening van een bankrekening) of wanneer ze worden verzameld via apparaten of technologieën voor het observeren van de activiteit van individuen

(voorbeelden: analyse van internetnavigatie, geolocatie en Wi-Fi-analyse / tracking voor publieksmeting, enz.);
    - en **in het geval van indirecte verzameling van persoonsgegevens**, wanneer gegevens niet rechtstreeks van personen worden verzameld (voorbeelden: gegevens die zijn opgehaald bij handelspartners, gegevensmakelaars, openbaar beschikbare bronnen of andere).

- Deze informatie is nodig:
    - **tijdens de gegevensverzameling** in het geval van directe verzameling;
    - **zo snel mogelijk in geval van indirecte inzameling** (in het bijzonder op het moment van het eerste contact met de persoon) en uiterlijk een maand na de afhaling (met uitzonderingen);
    - **in het geval van een substantiële wijziging of een bepaalde gebeurtenis**. Bijvoorbeeld: nieuw doel, nieuwe ontvangers, verandering in de manier waarop rechten worden uitgeoefend, datalek.

13.2. Welke informatie moet ik geven?

- In alle gevallen moet je het volgende opgeven:
    - **De identiteit en contactgegevens van de organisatie** die de gegevens verzamelt (wie verwerkt de gegevens?);
    - **De doeleinden** (waarvoor worden de verzamelde gegevens gebruikt?);
    - **De wettelijke basis** waarop de gegevensverwerking is gebaseerd (vind alle informatie op de wettelijke basis);
    - **Het verplichte of facultatieve karakter van de gegevensverzameling** (wat een voorafgaande reflectie impliceert over het nut van het verzamelen van de gegevens in het licht van het nagestreefde doel - het beginsel van "minimalisering" van de gegevens) en de **gevolgen voor de persoon** in geval van niet-verstrekking van de gegevens;
    - **Ontvangers of categorieën ontvangers van de gegevens** (wie moet ze openen of ontvangen voor de gedefinieerde doeleinden, inclusief verwerkers?);
    - **De bewaartermijn van gegevens** (of criteria om deze te bepalen);
    - **Het bestaan van de rechten van betrokkenen en de middelen om deze uit te oefenen** (het recht op toegang, rectificatie, wissing en beperking is van toepassing op alle verwerkingen);
    - **de contactgegevens van de functionaris voor gegevensbescherming** van het orgaan, indien aangesteld, of van een contactpunt voor kwesties in verband met de bescherming van persoonsgegevens;
    - **Het recht om een klacht in te dienen bij je lokale agentschap voor gegevensbescherming**.

- In bepaalde specifieke gevallen moet aanvullende informatie worden verstrekt, bijvoorbeeld in het geval van gegevensoverdrachten buiten de EU, volledig geautomatiseerde besluitvorming of profilering, of wanneer de wettelijke basis voor de verwerking het legitieme belang is dat wordt nagestreefd door de instantie die de gegevens verzamelt (zie de richtsnoeren inzake transparantie voor meer informatie).

- In het geval van indirecte inzameling moet het volgende worden toegevoegd:
    - **Categorieën van** verzamelde gegevens;
    - **De bron van de gegevens** (waarbij met name wordt aangegeven of deze afkomstig zijn van openbaar beschikbare bronnen).

13.3. In welke vorm moet ik deze informatie verstrekken?

- De informatie moet **gemakkelijk toegankelijk** zijn: de gebruiker moet deze zonder problemen kunnen vinden.

- **Het moet op een duidelijke en begrijpelijke manier worden verstrekt**, d.w.z. met een eenvoudige woordenschat (korte zinnen, geen juridische of technische termen, geen dubbelzinnigheden) en informatie die is aangepast aan de doelgroep (met bijzondere aandacht voor kinderen en kwetsbare personen).

- **Het moet op een beknopte manier worden geschreven**. Om de valkuil van een stortvloed aan informatie die de gebruiker overstemt te voorkomen, is het noodzakelijk om **de meest relevante informatie op het juiste moment te brengen**.

- Gegevensbeschermingsgerelateerde informatie moet te **onderscheiden zijn van informatie die niet specifiek verband houdt met privacy (zoals contractuele clausules of algemene gebruiksvoorwaarden).**

13.4. Welke communicatie moet worden gemaakt wanneer de gegevensbeveiliging in het gedrang komt?

- **Een organisatie kan per ongeluk of nalatig lijden, per ongeluk of kwaadwillig, aan een inbreuk op persoonsgegevens, d.w.z. de vernietiging, het verlies, de wijziging of ongeoorloofde openbaarmaking van gegevens**. In dit geval moet de organisatie de schending binnen 72 uur melden aan de lokale instantie voor gegevensbescherming als deze waarschijnlijk een risico vormt voor de rechten en vrijheden van individuen.

- Indien deze risico's hoog zijn, moet de organisatie de betrokken personen ook zo snel mogelijk informeren en hen advies geven over hoe ze hun gegevens kunnen beschermen (bv. annulering van een gecompromitteerde bankkaart, wijziging van een wachtwoord, wijziging van privacy-instellingen, enz.).

- Kennisgeving van de overtreding aan de AP moet worden gedaan via de website van de AP.

13.5. Nuttige bronnen

- De Data &Design site ontwikkeld door het Digital Innovation Laboratory van de CNIL ontwikkelt deze concepten en bevat interface voorbeelden.

- De CNIL-site bevat ook veel voorbeelden van informatieberichten in het Frans.

- De pagina over schendingen van persoonsgegevens op de website van de CNIL (in het Frans).

14. Bereid je voor op de uitoefening van de rechten van mensen

De personen van wie je de gegevens verwerkt, hebben rechten op zijn of haar gegevens: recht op toegang, rectificatie, bezwaar, wissing, gegevensoverdraagbaarheid en beperking van de verwerking. Je moet hen de middelen geven om hun rechten effectief uit te oefenen en in je computersystemen de technische hulpmiddelen verstrekken waarmee naar behoren rekening kan worden gehouden met hun rechten.

Door van tevoren voor te bereiden hoe zij contact met je zullen opnemen en hoe je met hun verzoeken zult omgaan, kan je de uitoefening van deze rechten effectief beheren.

14.1. Minimaal in te voeren maatregelen

- Alle organisaties die persoonsgegevens gebruiken, hebben **de verplichting om aan te geven waar en hoe** individuen hun rechten met betrekking tot deze gegevens kunnen uitoefenen. Je kunt bijvoorbeeld een e-mailadres of een webformulier vermelden bij het informeren van personen, evenals in je privacybeleid.

- Om de uitoefening van de rechten van mensen te vergemakkelijken, kunnen deze rechten ook geheel of gedeeltelijk rechtstreeks in **de applicatie of software die je ontwikkelt,** worden **geïmplementeerd**. Deze specifieke implementatie is niet verplicht, maar stelt je in staat om aan de verwachtingen van gebruikers te voldoen en de tijd en complexiteit van het verwerken van dit soort verzoeken te verminderen.

- Vergeet vooral niet om in geval van toegang of bewerkingen die rechtstreeks worden uitgevoerd door een persoon die zijn of haar rechten uitoefent, zijn **authenticatie op** een veilige manier te beheren. Traceer over het algemeen ook alle bewerkingen die een impact hebben op zijn of haar persoonlijke gegevens.

14.2. Hier zijn enkele voorbeelden van rechten en hun mogelijke implementatie

- **Recht op toegang**: mensen hebben het recht om een kopie te verkrijgen van alle informatie die je over hen hebt. Hierdoor kan een persoon onder andere weten of er gegevens over hem of haar worden verwerkt en een leesbare kopie in een begrijpelijk formaat verkrijgen. Het maakt het met name mogelijk om de juistheid van de gegevens te controleren.

  Mogelijke implementatie: Zorg voor een functionaliteit om alle gegevens met betrekking tot een persoon weer te geven. Als er veel gegevens zijn, kan je de gegevens opsplitsen in verschillende weergaven. Als de gegevens te groot zijn, bied de persoon dan aan om een archief te downloaden met al zijn of haar gegevens.

- **Recht op verwijdering**: Personen hebben het recht om te verzoeken om verwijdering van alle gegevens die je over hen bewaart.

  Mogelijke implementaties:

  1. Een functionaliteit bieden om alle gegevens met betrekking tot een persoon te wissen.

  2. Zorg ook voor automatische kennisgeving aan verwerkers om ook de gegevens met betrekking tot die persoon te wissen.

  3. Zorg ook voor gegevensverwijdering in back-ups of bied een alternatieve oplossing die gewiste gegevens met betrekking tot die persoon niet herstelt.

- **Recht op bezwaar**: individuen hebben het recht om in bepaalde gevallen bezwaar te maken tegen het gebruik van hun gegevens voor een specifiek doel.

  Mogelijke implementatie: een functionaliteit bieden waarmee de betrokkene bezwaar kan maken tegen de verwerking. Wanneer de betrokkene zijn of haar recht om op deze manier bezwaar te maken uitoefent, moet de voor de verwerking verantwoordelijke reeds verzamelde gegevens verwijderen en vervolgens geen gegevens meer verzamelen die betrekking hebben op die persoon.

- **Recht op gegevensportabiliteit**: Individuen hebben het recht om hun gegevens op te halen in een machineleesbaar formaat voor eigen gebruik of voor overdracht naar een andere organisatie.

  Mogelijke implementatie: Zorg voor een functie waarmee de betrokkene zijn of haar gegevens kan downloaden in een standaard machineleesbaar formaat (CSV, XML, JSON, enz.).

- **Recht op rectificatie**: Individuen hebben het recht om de wijziging van hun gegevens te vragen wanneer deze onjuist zijn om het gebruik of de verspreiding van onjuiste informatie te beperken.

  Mogelijke implementatie: Sta toe om gegevens rechtstreeks in het gebruikersaccount te wijzigen.

- **Recht op beperking van de verwerking**: personen hebben het recht om te verzoeken dat de verwerking van hun gegevens gedurende een bepaalde periode wordt geblokkeerd, bijvoorbeeld de tijd om een geschil van hun kant met betrekking tot het gebruik van hun gegevens te onderzoeken of een verzoek om rechten uit te oefenen.

  Mogelijke implementatie: Laat beheerders gegevens over een persoon in "quarantaine" plaatsen: deze gegevens kunnen dan niet meer worden gelezen of gewijzigd.

14.3. Tot slot

- De Data &Design site ontwikkeld door het Digital Innovation Laboratory van de CNIL ontwikkelt deze concepten en bevat voorbeelden van interfaces voor het uitoefenen van rechten.

- Tot slot, wees **inventief**! (Vraag bij twijfel om advies).

15. Definieer een bewaartermijn voor gegevens

Persoonsgegevens kunnen niet voor onbepaalde tijd worden bewaard: dit moet worden gedefinieerd in overeenstemming met de doeleinden van de verwerking. Zodra dit doel is bereikt, moeten de gegevens worden gearchiveerd, verwijderd of anoniem worden gemaakt (bijvoorbeeld om statistieken te produceren).

15.1. Cycli voor het bewaren van gegevens

- De bewaarcyclus voor persoonsgegevens kan worden onderverdeeld in **drie verschillende opeenvolgende fasen**:
    - De actieve database;
    - Tussentijdse archivering;
    - Definitieve archivering of verwijdering.

- De mechanismen voor het verwijderen van persoonsgegevens uit de actieve bases zorgen ervoor dat de gegevens door de operationele diensten alleen worden bewaard en toegankelijk zijn **voor de tijd die nodig is om het doel van de verwerking te bereiken**.

- Zorg ervoor dat **gegevens niet in actieve databases worden bewaard** door ze simpelweg **als gearchiveerd te noteren**. De gearchiveerde gegevens (tussenliggend archief) mogen alleen toegankelijk zijn voor een specifieke dienst die verantwoordelijk is voor de toegang tot en het verwijderen ervan uit het archief indien nodig.

- Zorg er ook voor dat je **toegangsmodi hebt opgegeven** voor de gearchiveerde gegevens, omdat het gebruik van een archief op ad-hoc- en uitzonderlijke basis moet zijn.

- Gebruik indien mogelijk dezelfde implementatie bij de implementatie van de **gegevenszuivering of anonimisering** als degene die het **recht op verwijdering** beheert (zie Hoofdstuk 14 over de uitoefening van rechten), om een homogene werking van je systeem te garanderen.

16. Houd rekening met de wettelijke basis bij de technische uitvoering

De verwerking van persoonsgegevens moet gebaseerd zijn op een van de "rechtsgronden" genoemd in artikel 6 van de AVG. De rechtsgrondslag van een verwerking is in zekere zin de rechtvaardiging van het bestaan van de verwerking. De keuze van een rechtsgrondslag heeft een directe impact op de voorwaarden voor de uitvoering van de verwerking en de rechten van individuen (zie Hoofdstuk 14). Het anticiperen op de wettelijke basis van de verwerkingen voorafgaand aan een ontwikkeling zal je dus helpen de nodige functies te integreren om ervoor te zorgen dat deze verwerkingen voldoen aan de wet en de rechten van het individu respecteren.

16.1. Definitie van de rechtsgrondslagen in de AVG

- In het kader van een ontwikkeling voor een particuliere organisatie (bedrijven, verenigingen, enz.) wordt vaak de volgende rechtsgrondslag gebruikt:
    - **Het contract**: de verwerking is noodzakelijk voor de uitvoering of voorbereiding van een contract tussen de betrokkene en de instantie die de verwerking uitvoert;
    - **Het gerechtvaardigd belang**: de organisatie heeft een "gerechtvaardigd" belang bij het uitvoeren van de verwerking en het is niet waarschijnlijk dat het de rechten en vrijheden van de betrokkenen nadelig zal beïnvloeden;
    - **Toestemming**: de betrokkene heeft zijn of haar uitdrukkelijke toestemming gegeven voor de verwerking.

- Als je een overheidsinstantie of een orgaan bent dat taken van algemeen belang uitvoert, kunnen ook andere rechtsgrondslagen worden gebruikt:
    - **De wettelijke verplichting**: de verwerking wordt opgelegd door regelgevende teksten.
    - **De taak van algemeen belang**: de verwerking is noodzakelijk voor de uitvoering van een taak van algemeen belang.

- Ten slotte kan in zeer specifieke gevallen **de bescherming van vitale belangen** als rechtsgrondslag worden gebruikt, bijvoorbeeld wanneer verwerking noodzakelijk is om de verspreiding van epidemieën te volgen of in geval van humanitaire noodsituaties.

16.2. Kies de juiste rechtsgrondslag

- Controleer eerst of **een tekst geen specifieke beperkingen oplegt** (bijvoorbeeld: cookies en andere trackers).

- **Voor een bepaald doel mag slechts één rechtsgrondslag worden gekozen**. De rechtsgrondslag kan niet voor hetzelfde doel worden gecumuleerd. Dezelfde gegevensverwerking kan verschillende doeleinden nastreven en voor elk van hen moet dan een rechtsgrondslag worden gedefinieerd.

- Zoals hierboven vermeld, als je een **overheidsinstantie bent**, zullen de wettelijke verplichting en de taak van algemeen belang in de meeste gevallen het meest

relevant zijn.

- Als je verwerking deel uitmaakt van een contractuele relatie en het doel ervan objectief en strikt noodzakelijk is voor de levering van de service van de gebruiker (bijv. naam, voornaam en adres om een account aan te maken op een e-commercesite), dan **moet het contract geschikt zijn**.

- Als je verwerking geen deel uitmaakt van een contractuele relatie met de gebruiker, kan **de wettelijke basis van toestemming of legitiem belang** worden ingeroepen. Als uw verwerking mogelijk indringend is (profilering, verzameling van geolocatiegegevens, enz.), dan is toestemming waarschijnlijk de juiste rechtsgrondslag.

- Als je verwerking gevoelige gegevens bevat (gezondheidsgegevens, gegevens over leven of seksuele geaardheid, enz.), dan moet je, naast de rechtsgrondslag, een uitzondering identificeren waarin artikel 9 van de AVG voorziet.

16.3. Uitoefening van rechten en modaliteiten van informatie die volgens de rechtsgrondslag moet worden verstrekt

- De volgende tabel geeft een overzicht van de uitoefening van de rechten die overeenkomstig de rechtsgrondslag moeten worden verleend:

	Recht op inzage	Recht op rectificatie	Recht op gegevenswissing	Recht op beperking van de verwerking	Recht op gegevensoverdraagbaarheid	Recht van bezwaar
Toestemming	✓	✓	✓	✓	✓	**Toestemming intrekken**
Contract	✓	✓	✓	✓	✓	✗
Gerechtvaardigd belang	✓	✓	✓	✓	✗	✓
Wettelijke verplichting	✓	✓	✗	✓	✗	✗
Algemeen belang	✓	✓	✗	✓	✗	✓
Bescherming van vitale belangen	✓	✓	✓	✓	✗	✗

- De gebruikte rechtsgrondslag moet **altijd worden vermeld in de informatie die aan de persoon wordt doorgegeven**.

- **Wanneer je verwerking is gebaseerd op legitiem belang**, moet je ook de nagestreefde legitieme belangen aangeven (bestrijding van fraude, systeembeveiliging, enz.).

- Het wordt aanbevolen om **je keuze van wettelijke basis te documenteren**. Deze keuzes kunnen bijvoorbeeld worden aangegeven in een verwerkingskaart of worden gekoppeld aan uw technische documentatie.

16.4. Het specifieke geval van cookies en andere trackers

- De Europese ePrivacy-richtlijn vereist de toestemming van de gebruiker voordat enige actie wordt ondernomen om informatie op te slaan - via cookies, id's of andere tracers (software-vingerafdrukken, pixels) of om toegang te krijgen tot informatie die is opgeslagen in de eindapparatuur van de gebruiker.

- Er wordt echter een uitzondering gemaakt wanneer cookies uitsluitend bedoeld zijn voor het uitvoeren van elektronische communicatie, of strikt noodzakelijk zijn om een door de gebruiker gevraagde dienst te leveren.

- Bovendien is het gebruik van een enkele tracer voor meerdere doeleinden niet vrijgesteld van het verkrijgen van toestemming voor de doeleinden die dit vereisen. Als een authenticatiecookie bijvoorbeeld ook wordt gebruikt voor reclametargetingdoeleinden, moet toestemming worden verkregen voor het laatste doel, op dezelfde manier als voor een niet-geregistreerde site.

17. Gebruik analytics op je websites en applicaties

Hulpmiddelen voor publieksmeting worden gebruikt om informatie te verkrijgen over de navigatie van bezoekers op een website of mobiele applicatie. In het bijzonder maken ze het mogelijk om te begrijpen hoe gebruikers op een site aankomen en om hun reis te reconstrueren. Met behulp van cookies zijn ze onderworpen aan de regel van toestemming, behalve in één specifiek geval. Houd er rekening mee dat dit gedeelte betrekking heeft op de ePrivacy-richtlijn en onderhevig kan zijn aan nationale variaties. Neem contact op met je lokale agentschap voor gegevensbescherming om zijn positie te kennen.

17.1. Toestemming verkrijgen

- Over het algemeen moeten redacteuren van sites of applicaties, **voordat ze een cookie of tracer plaatsen of lezen**:
    - internetgebruikers te informeren over het doel van cookies;
    - hun toestemming te verkrijgen;
    - geef hen een middel om hen te weigeren.

- Tenzij ze precies binnen de hieronder gedefinieerde perimeter vallen, **geldt deze verplichting voor tracers die worden gebruikt voor publieksmeting**.

17.2. Om te profiteren van de vrijstelling van toestemming

- **Onder een aantal voorwaarden** zijn cookies die worden gebruikt voor publieksmeting vrijgesteld van toestemming.

- **Deze voorwaarden, zoals gespecificeerd in de richtlijnen voor cookies en andere trackers, zijn**:
    - Om gebruikers te informeren over hun gebruik;

    - Om hen de mogelijkheid te geven bezwaar te maken tegen het gebruik ervan;
    - Beperken tot de volgende doeleinden:
        - publieksmeting;
        - A/B-testen;
    - De verwerkte gegevens niet te vergelijken met andere verwerkingen (klantenbestanden, statistieken over bezoeken aan andere sites, enz.);
    - Om het bereik van de tracer te beperken tot één site of toepassingseditor;
    - Om de laatste byte van het IP-adres af te korten;
    - Om de levensduur van de trackers te beperken tot 13 maanden.

- Mits aan de voorwaarden is voldaan, **schakelen we daarom over van een opt-in naar een opt-out regime**.

- Het is ook mogelijk voor dezelfde derde partij (onderaannemer) om een vergelijkende publieksmetingsdienst aan te bieden aan meerdere uitgevers, op voorwaarde dat **de gegevens onafhankelijk van elkaar worden verzameld, verwerkt en opgeslagen voor elke uitgever en dat de trackers onafhankelijk van elkaar zijn**.

17.3. In de praktijk

- **De meeste meetaanbiedingen voor grote doelgroepen vallen niet onder het toepassingsgebied van de vrijstelling, ongeacht hun configuratie**.

- Om van deze vrijstelling te profiteren, neem je contact op met je oplossingsprovider of gebruik je open source-software zoals Matomo die je zelf kunt configureren.