Privacyontwerpstrategieën
(Het Blauwe Boekje)

Jaap-Henk Hoepman

27 januari 2020

1 Inleiding

We willen zelf bepalen welke persoonlijke details we met anderen delen, en hoe ze gebruikt worden. Dat niet iedereen meteen weet wat we doen of wat we denken. Dat onze baas niet weet wat we met onze vrienden bespreken. Dat persoonlijke informatie niet buiten de oorspronkelijke context verkeerd geïnterpreteerd wordt. We willen een beetje privacy dus. Maar dat is steeds minder vanzelfsprekend in een wereld waarin digitale innovaties ons steeds meer omringen en steeds dichter op de huid zitten.

Privacy is dus belangrijk. Het biedt bescherming tegen opdringerige bedrijven of een alwetende overheid. Doel is de machtsbalans tussen individu en maatschappij in evenwicht te houden. Dit is in een democratische rechtstaat niet alleen een individueel belang, maar ook een maatschappelijk belang. Privacy is daarom een grondrecht. Strenge Europese wetten beschermen de privacy van alle mensen op Europees grondgebied.

Helaas is deze wetgeving complex en vaag. Ze biedt weinig concrete handvatten voor ontwerpers en systeembouwers. Dat is een probleem als je een systeem privacy vriendelijk wilt ontwerpen. Bijvoorbeeld door de *privacy by design* ontwerpfilosofie toe te passen, die vereist dat privacybescherming vanaf het begin af aan meegenomen wordt bij het ontwerpen en bouwen van nieuwe systemen. Privacy wordt daarmee, net als beveiliging, een softwarekwaliteitsattribuut. Privacy by design is vanaf 2018 wettelijk verplicht. Maar je kunt het ook gebruiken om verder te gaan dan de minimale bescherming die de wet vereist, bijvoorbeeld door te innoveren op basis van privacy.

Maar hoe maak je privacy by design concreet? En hoe pas je het in de praktijk toe? Daar geeft dit boek antwoord op.

Er zijn allerlei privacy beschermende technologieën, maar die zijn pas van toepassing als je een systeem gaat implementeren. Je hebt er weinig aan als je begint na te denken over wat het systeem moet kunnen en hoe je dat zou kunnen realiseren op een privacy vriendelijke manier.

Waar en hoe moet je beginnen?

Privacyontwerpstrategieën geven hierop een antwoord. Ze vertalen vage juridische eisen in concrete ontwerpeisen. Ze formuleren onderwerpen

voor de discussie over hoe het te ontwerpen systeem er uit moet zien. Ze sturen de eerste ontwerpschetsen in een privacy vriendelijke richting, door in het begin te dwingen weloverwogen principiële keuzes te maken.

1.1 Voor wie is dit boek?

Dit boek is gericht op alle organisaties (bedrijfsleven of overheid) die persoonsgegevens verwerken. Zij is met name bedoeld voor ontwerpers en bouwers van systemen die persoonsgegevens verwerken, en de mensen die voor die systemen verantwoordelijk zijn.

1.2 Leeswijzer

Dit boek beschrijft de acht privacyontwerpstrategieën. Iedere strategie wordt kort uitgelegd en geïllustreerd aan de hand van praktische voorbeelden. Daarnaast worden een aantal concrete technieken genoemd waarmee de strategie in de praktijk geïmplementeerd kan worden.

In het twee na laatste hoofdstuk gaan we in op de vraag hoe je de privacyontwerpstrategieën in de praktijk toepast, en hoe ze ingepast kunnen worden in bestaande ontwikkelmethodes.

Als je meer wilt weten over privacy in het algemeen en privacy by design in het bijzonder: achterin dit boek staan verwijzingen naar boeken, websites en andere bronnen met meer informatie. Ook kun je daar vinden hoe je op de hoogte kunt blijven van de laatste ontwikkelingen.

We sluiten af met een verklarende woordenlijst.

1.3 Dankwoord

Ik wil graag Gergely Alpár bedanken voor zijn suggesties.

2 De acht privacyontwerpstrategieën

Er zijn in totaal acht privacyontwerpstrategieën te onderscheiden. Ze zijn onderverdeeld in twee groepen: data georiënteerde strategieën en proces georiënteerde strategieën.

De data georiënteerde strategieën zijn gericht op de privacy vriendelijke verwerking van de data zelf. Ze zijn dus technisch van aard. Er zijn er vier.

Minimaliseer (Minimise)
: Beperk zo veel mogelijk de verwerking van persoonsgegevens.

Scheid (Separate)
: Scheid de verwerking van persoonsgegevens zo veel mogelijk van elkaar.

Abstraheer (Abstract)
: Beperk zoveel mogelijk het detail waarin persoonsgegevens worden verwerkt.

Verberg (Hide)
: Bescherm persoonsgegevens, of maak ze onherleidbaar of onobserveerbaar. Voorkom dat persoonsgegevens openbaar worden.

De proces georiënteerde strategieën zijn gericht op de processen rond de verwerking van persoonsgegevens. Ze gaan over de organisatorische aspecten en de noodzakelijke procedures. We onderscheiden de volgende vier.

Informeer (Inform)
: Informeer gebruikers over de verwerking van hun persoonsgegevens.

Geef controle (Control)
: Geef gebruikers controle over de verwerking van hun persoonsgegevens.

Dwing af (Enforce)
: Committeer je aan een privacy vriendelijke verwerking van persoonsgegevens, en dwing deze af.

Toon aan (Demonstrate)
: Toon aan dat je op een privacy vriendelijke wijze persoonsgegevens verwerkt.

Binnen een strategie onderscheiden we een aantal *tactieken* die ieder op een duidelijk andere wijze invulling geven aan de overkoepelende strategie. In de volgende acht hoofdstukken beschrijven kort we elk van de strategieën, en de bijbehorende tactieken, en geven voorbeelden van hoe ze in de praktijk toegepast kunnen worden.

3 Minimaliseer

Beperk zo veel mogelijk de verwerking van persoonsgegevens.

De meest voor de hand liggende strategie om privacy te beschermen is het minimaliseren van persoonsgegevens. Met gegevens die je niet verwerkt kan niets mis gaan: ze kunnen niet misbruikt worden, verkeerd gebruikt worden, of per ongeluk openbaar gemaakt worden. Denk goed na over de gegevens die je nodig hebt. Soms kan een radicaal andere benadering er toe leiden dat je veel minder of misschien wel helemaal geen persoonsgegeven hoeft te verwerken.

3.1 Tactieken

Minimaliseren van persoonsgegevens kan door van minder personen gegevens te verwerken, of per persoon minder gegevens te verwerken. Een aantal verschillende tactieken zijn van toepassing.

Selecteer (select) Selecteer alleen relevante personen of gegevens. Bepaal van te voren welke personen of gegevens relevant zijn, en verzamel enkel die gegevens. Bewaar binnenkomende gegevens alleen als ze aan het selectiecriterium voldoen. Wees conservatief in je selectiecriteria: selecteer alleen dat wat strikt noodzakelijk is. Gebruik een whitelist.

Sluit uit (exclude) Sluit op voorhand bepaalde personen of gegevens uit. Bepaal van te voren welke personen of gegevens niet relevant zijn, en verzamel die gegevens niet, of gooi ze meteen weg als ze onverhoopt toch binnen komen. Wees ruim in je uitsluitingsgronden: sluit zo veel mogelijk gegevens uit, tenzij je zeker weet, en kunt verantwoorden, dat je ze nodig hebt. Gebruik een blacklist.

Verwijder (strip) Verwijder (deel)gegevens die niet langer nodig zijn. Bepaal van te voren hoe lang gegevens nodig zijn, en zorg dat ze automatisch na die tijd verwijderd worden. Als het een specifiek veld uit een record betreft dat verder nog wel bewaard moet worden, zet dat veld dan op een default waarde. Veranderingen in de organisatie, het dienstportfolio of een wijziging in een proces kunnen er

ook toe leiden dat gegevens niet langer relevant zijn.

Vernietig (destroy) Verwijder volledige persoonsgegevens zodra ze niet langer nodig zijn. Zorg dat de gegevens ook echt niet meer beschikbaar zijn. Dat wil zeggen: verwijder gegevens ook van eventuele backups, en wis data op harde schijven en andere opslagmedia op een veilige manier.

Minimalisatie wordt ook bereikt door je te richten op kernactiviteiten en bedrijfsvreemde activiteiten te vermijden.

> ING wou in 2014 bedrijven de mogelijkheid geven gerichte reclame aan rekeninghouders te sturen op basis van hun persoonlijke transactiegegevens. Dit leidde tot een storm van protest. Voor dergelijke gerichte reclame moet op basis van de transactiegegevens nieuwe informatie over de persoonlijke voorkeuren van de klant afgeleid worden. Deze nieuwe persoonsgegevens heeft de bank niet nodig voor het uitvoeren van haar kernactiviteiten.

3.2 Voorbeelden

Het uitsluiten en selecteren van gegevens is niet alleen relevant als gegevens verzameld worden of op een andere manier binnenkomen, maar ook bij het gebruik van reeds verzamelde gegevens. Zorg ervoor dat interne processen en applicaties enkel gegevens gebruiken die relevant zijn voor het proces. Zorg dat alleen echt relevante gegevens gedeeld worden met andere in- of externe partijen. En let goed op als tijdens de verwerking van gegevens nieuwe gegevens ontstaan: selecteer of sluit ook dan uit welke nieuwe gegevens noodzakelijk zijn.

> *Data mining, deep learning of andere Big Data technieken genereren nieuwe inzichten. Selecteer alleen die inzichten die relevant zijn. Gooi ander gegevens weg, en bewaar die niet onder het motto "baat het niet dan schaadt het niet": het schaadt soms wel degelijk.*

Met andere woorden, ook bij het gebruiken, delen, analyseren en verrijken van gegevens moet je scherp zijn op minimaliseren.

Het verschil tussen verwijderen en vernietigen is subtiel: verwijderen speelt vooral een rol op de applicatielaag, terwijl vernietigen zich richt op de fysieke opslagmedia.

Er bestaan geteste en goedkeurde methode om data op een harde schijf écht te vernietigen (bijvoorbeeld door de sectoren een aantal keren met willekeurige data te overschrijven). Een efficiënte methode om data op backups te vernietigen is om de data te versleutelen voordat de backup gemaakt wordt. Door bepaalde sleutels met een bepaalde bewaarperiode te associëren kan alle data voor die periode simpelweg vernietigd worden door deze specifieke sleutel te vernietigen.

Een radicaal andere systeemarchitectuur kan een veel privacyvriendelijker systeem opleveren. Rekeningrijden (waarbij het te betalen tarief afhangt van de plaats en tijd waar het voertuig zich bevindt) is hiervan een mooi voorbeeld. Het kan eenvoudig geïmplementeerd worden als ieder voertuig in Nederland continue aan de Belastingdienst doorgeeft waar deze zich bevindt. De privacy implicaties zijn in dat geval enorm. Een andere optie is om in ieder voertuig een slim kastje te plaatsen dat op basis van een vooraf ingestelde tariefkaart het te betalen bedrag bepaalt. De som van al deze kleine bedragen wordt dan aan het eind van de maand aan de Belastingdienst verstuurd. In dat geval zijn de privacy implicaties van rekeningrijden beperkt.

4 Scheid

Scheid de verwerking van persoonsgegevens zo veel mogelijk van elkaar.

Een andere belangrijke strategie is om verschillende persoonsgegevens gescheiden (logisch dan wel fysiek) van elkaar te verwerken. Dit maakt het moeilijker om verschillende gegevens met elkaar te combineren. Door gegevens uit verschillende contexten apart te verwerken, is het risico kleiner dat gegevens uit de ene context in de andere context bekend worden. Helemaal als deze scheiding fysiek is. Gescheiden verwerking geeft invulling aan het concept “contextual integrity”.

4.1 Tactieken

Gescheiden verwerking van persoonsgegevens kan middels twee verschillende tactieken bereikt worden.

Isoleer (isolate) Verzamel of verwerk persoonsgegevens in verschillende, logisch gescheiden, databases of systemen.

Distribueer (distribute) Distribueer de verwerking over verschillende fysieke locaties. Doe zoveel mogelijk in de apparatuur (PC, smartphone) van de eindgebruiker, en maak zo weinig mogelijk gebruik van centrale componenten. Maak gebruik van decentrale of zelfs gedistribueerde systemen in plaats van gecentraliseerde architecturen.

4.2 Voorbeelden

Een sociaal netwerk stelt mensen in staat om berichten en foto’s met vrienden en bekenden te delen. Huidige sociale netwerken (Twitter, Facebook) zijn centrale architecturen: het platform ziet alles wat de gebruikers met elkaar delen. Dat bepaalt ook de (hoge) waarde van het sociale netwerk, en is ook waarop het businessmodel op gebaseerd is. Een privacyvriendelijke versie van een sociaal netwerk zou gebruikers hun profielen en statusupdates lokaal op hun eigen smartphone laten opslaan en op een peer-to-peer manier openstellen voor hun vrienden en bekenden. Er

zou in dit geval geen enkele data centraal opgeslagen of verwerkt hoeven worden.

In het algemeen kunnen peer-to-peer netwerken en gedistribueerde algoritmen gebruikt worden in plaats van centralistische oplossingen, om de privacy bescherming te vergroten.

> *Een spaarbankboekje is hiervan een mooi voorbeeld. In zo'n boekje werd het saldo van de spaarrekening bijgehouden. Bij iedere storting of opname moest het spaarbankboekje mee naar de bank, om het saldo bij te werken. Dat saldo, en de houder, waren dus (in theorie) niet bekend bij de bank. (In de praktijk zal de bank een schaduwboekhouding hebben bijgehouden.) Een spaarbankboekje was dus een soort anonieme spaarrekening.*

Apple's iOS 10 maakt het mogelijk om foto's te groeperen naar de personen die op de foto staan. Daar wordt gezichtsherkenningssoftware voor gebruikt. In iOS 10 draait deze software lokaal op de telefoon van de gebruiker. De foto's worden dus niet voor analyse naar een centrale server gestuurd.

Een extreem privacyvriendelijke manier van het decentraal verwerken van gegevens is *secure multiparty computation*. Met deze techniek kan een functie over de invoer van een groot aantal verschillende apparaten berekend worden zonder dat deze waarden het apparaat verlaten. Op deze manier zijn bijvoorbeeld in Denemarken veilige en privacy vriendelijke veilingen gehouden. Ieder bod bleef geheim, behalve het hoogste bod: dat kon wel bepaald worden.

5 Abstraheer

Beperk zoveel mogelijk het detail waarin persoonsgegevens worden verwerkt.

Daar waar minimaliseren zich richt op de fundamentele keuze om bepaalde informatie over bepaalde personen al dan niet te verwerken, richt abstraheren zich op de subtielere vraag in welke mate van detail persoonsgegevens verwerkt moeten worden. Hoe minder details verwerkt worden, hoe meer we 'uitzoomen', des te lager het privacyrisico is.

5.1 Tactieken

Het in mindere mate van detail verwerken van persoonsgegevens kan op subject dan wel attribuut niveau plaatsvinden. De volgende drie tactieken zijn van toepassing.

Groepeer (group) Aggregeer informatie over categorieën personen in plaats van ieder individu. Stel een groepsprofiel op (met de gemiddelde waarde van de gegevens van alle mensen van een bepaalde leeftijd of een bepaald postcode gebied).

Vat samen, generaliseer (summarize) Vat gedetailleerde informatie samen in meer algemene gegevens. Registreer bijvoorbeeld een leeftijdscategorie in plaats van een geboortedatum, of een woonplaats in plaats van het precieze adres.

Ruis toevoegen, verstoren (perturb) Gebruik niet de precieze waarde van een gegeven. Gebruik een benadering van de waarde, of pas de waarde aan met een kleine hoeveelheid ruis.

Vaak is het zo dat de relevantie van gedetailleerde informatie na verloop van tijd afneemt. Daar waar gedetailleerde logbestanden noodzakelijke zijn om in geval van een storing of een hack direct in te kunnen grijpen, is na een paar maanden het wellicht voldoende om enkel het aantal gebruikers van een dienst (eventueel uitgesplitst naar regio of specifieke dienstonderdelen) te bewaren. Wees hier alert op en schoon bestanden of databases op.

Merk overigens op dat ook groepsgebaseerde profielen een privacy risico opleveren als van een individu eenvoudig is vast te stellen of deze tot de groep behoort (zoals mensen met een bepaalde aandoening, of mensen met een bepaald financieel risicoprofiel).

5.2 Voorbeelden

In veel gevallen (denk aan speciale regelingen voor senioren of jongeren, of voor het controleren of iemand meerderjarig is) is alleen de leeftijd en niet de specifieke geboortedatum van belang. In plaats van de geboortedatum te registreren volstaat dan het attribuut "ouder dan 18" of "65+".

Slimme meters zijn een voorbeeld van systemen die zowel in de *ruimte* als in de *tijd* abstraheren. Voor stabiliteit van het elektriciteitsnetwerk is het gedetailleerde verbruik van één huishouden niet relevant. Het is voldoende om in realtime het verbruik over een straat of wijk te kunnen meten. Voor het bepalen van de rekening is realtime energieverbruik doorgeven niet noodzakelijk. Het volstaat om eens in de zoveel maanden het totale verbruik door te geven.

Homomorfe versleuteling maakt het mogelijk om te rekenen met versleutelde gegevens zonder de gegevens zelf te kennen. Zo kan een partij de som of het product van een aantal meetgegevens berekenen zonder ieder meetgegeven apart te kennen. Een andere partij kan vervolgens de som ontsleutelen voor verder gebruik. Zo komt niemand de individuele meetgegevens te weten.

Locatie gebaseerde diensten hebbend de locatie van de gebruiker nodig om relevante informatie (een restaurant in de buurt, bijvoorbeeld) te kunnen tonen. Maar afhankelijk van de dienst hoeft deze informatie niet altijd even nauwkeurig te zijn. Precieze GPS coördinaten zijn overbodig. Soms is een precisie van zeg een vierkante kilometer voldoende, waarna alle relevante gegevens voor dat grotere gebied naar de gebruiker worden gestuurd. Vervolgens wordt de meer gedetailleerde informatie lokaal er uit gefilterd.

Deze vorm van clusteren of verhullen (cloaking) geeft invulling aan het principe van k-anonimiteit. Dit principe vereist dat de data zo verhult wordt dat deze in principe op ten minste k verschillende mensen van toepassing kunnen zijn, die ieder ook in de dataset vertegenwoordigd

zijn, of van de dienst gebruik maken. Anders gezegd: naast jou zelf zijn er nog ten minste $k - 1$ andere gebruikers waarop de data van toepassing zouden kunnen zijn. Bij locatie gebaseerde diensten hangt k van de grootte van het gebied af, en het gemiddeld aantal personen dat zich normaal gesproken daar bevindt.

6 Verberg

Bescherm persoonsgegevens, of maak ze onherleidbaar of onobserveerbaar. Voorkom dat persoonsgegevens openbaar worden.

Deze belangrijke strategie richt zich op de vertrouwelijkheid, onherleidbaarheid en onobserveerbaarheid van persoonlijke gegevens. Dit in tegenstelling tot minimaliseren, dat zich richt op de expliciete keuze persoonsgegevens al dan niet te verwerken. Het afdoende beschermen van persoonsgegevens is een wettelijke vereiste.

6.1 Tactieken

De verberg strategie omvat daarom de volgende tactieken.

Beperk toegang (restrict) Beperk toegang tot persoonsgegevens. Zorg dat de informatiebeveiliging op orde is. Stel strikte maatregelen voor toegangscontrole op. Geef personen alleen toegang tot persoonsgegevens die ze strikt gesproken nodig hebben ('need to know'). Maak het moeilijk om met opzet of per ongeluk data te delen met onbevoegden.

Maak onbegrijpbaar (obfuscate) Maak data onbegrijpbaar voor derden. Versleutel data zodat ze onleesbaar worden zonder de sleutel. Hash persoonsgegevens, bijvoorbeeld om er pseudoniemen van te maken.

Verbreek link (dissociate) Verbreek de link en de correlatie tussen gebeurtenissen, personen en gegevens. Verwijder direct identificerende gegevens.

Meng (mix) Maak data of gebeurtenissen onherleidbaar, bijvoorbeeld door deze met elkaar te mengen, of te anonimiseren. Verberg gegevens in een 'wolk' van willekeurige andere gegevens. Verbreek de correlatie tussen twee gebeurtenissen, bijvoorbeeld door niet meteen te reageren. Verzamel eerst een aantal gebeurtenissen, of gegevens over een aantal personen, en verwerk deze dan in bulk.

Verbergen kan dus door persoonsgegevens te beschermen (je weet dat ze er zijn, maar je kunt er niet bij), onherleidbaar te maken (je weet welke

gegevens er zijn, alleen niet meer bij welke persoon die horen) of onobserveerbaar te maken (je bent je er niet eens van bewust dat er bepaalde gegevens zijn). Dit laatste aspect is vooral van toepassing op gedragsgegevens (metadata), dus bijvoorbeeld locatiegegevens, of de vraag wie met wie communiceert.

Vaak wordt een combinatie van deze tactieken gebruikt om gegevens te verbergen.

6.2 Voorbeelden

Hashing en versleuteling zijn standaard cryptografische technieken die je kunt gebruiken om persoonsgegevens te beveiligen. Gebruik dit zowel voor data die via het netwerk verstuurd wordt als bij data die wordt opgeslagen, en denk ook aan adequaat sleutelbeheer.

Sommige communicatie diensten en cloud diensten maken gebruik van end-to-end versleuteling. Hierbij spreken gebruikers van de dienst onderling, op een veilige wijze, cryptografische sleutels af. Die zijn niet bij die dienstaanbieder bekend. Hierdoor kan deze de gecommuniceerde of opgeslagen gegevens niet inzien. Die zijn alleen beschikbaar op de 'endpoints' (i.e. de smartphone of laptop) van de gebruikers zelf.

Attribute based credentials (ABCs) maken een privacy vriendelijke vorm van identiteitsbeheer mogelijk. Attributen zijn persoonlijke eigenschappen. Denk aan naam, leeftijd, gewicht, bloedgroep, inkomen, etc. Met ABCs kun je bewijzen dat je bepaalde attributen bezit, bijvoorbeeld dat je ouder bent dan achttien, zonder informatie over de rest vrij te geven. Sterker nog, ABCs zijn onlinkbaar: hergebruik van een credential is niet detecteerbaar. Als je honderd keer bij dezelfde dienstaanbieder aantoont dat je ouder bent dan achttien, dan is dat wat de dienstaanbieder betreft gebeurd door honderd verschillende personen.

Tor, the onion router, maakt websurfen anoniem. Je browser maakt niet direct contact met de webserver. De verbinding wordt opgezet via drie tussenliggende Tor nodes. Deze verbinding zijn versleuteld. Zo kan de webserver, je internet service provider, of een willekeurige derde partij (zelfs de Tor nodes) niet meer zien welke websites je bezoekt.

Merk op dat in de praktijk blijkt dat echt volledig geanonimiseerde ge-

gevens eigenlijk niet bestaan: vaak is uit de wel bewaarde gegevens met een redelijke mate van zekerheid de bijbehorende persoon te achterhalen. Vertrouw hier dus nooit helemaal op.

7 Informeer

Informeer gebruikers op tijd en adequaat over de verwerking van hun persoonsgegevens.

Transparantie over welke persoonsgegevens verwerkt worden, de manier waarop en met welk doel, is een essentiële stap naar betere privacybescherming. Het geeft gebruikers de mogelijkheid om goed geïnformeerd een beslissing te nemen over het al dan niet gebruiken van een dienst en het toestaan van de verwerking (zie de 'geef controle' strategie). Daarnaast geeft het samenleving als geheel de mogelijkheid om te controleren of organisaties verantwoordelijk met onze persoonsgegevens omgaan. ("Sunlight is said to be the best of disinfectants.")

7.1 Tactieken

Transparantie wordt bereikt door de volgende tactieken te volgen.

Informeer (supply) Vertel welke persoonsgegevens worden verwerkt, op welke manier deze worden verwerkt, en waarom. Geef aan hoe lang persoonsgegevens worden bewaard, en hoe ze verwijderd worden. Geef aan met wie persoonsgegevens worden gedeeld, welke afspraken daar over gemaakt zijn, en hoe je die afspraken controleert. Zet een link naar je privacybeleid op je homepagina, en in je app. Geef duidelijk aan hoe mensen contact op kunnen nemen.

Leg uit (explain) Leg uit welke persoonsgegevens worden verwerkt, en waarom. Beargumenteer waarom dit nodig is. Doe dit op een duidelijke en voor leken begrijpbare manier. Structureer je informatievoorziening en richt deze op verschillende doelgroepen: leken, experts, autoriteiten. Maak de informatie 'gelaagd': geef een overzicht en ga in aparte pagina's in op details.

Waarschuw (notify) Waarschuw gebruikers als hun persoonsgegevens gebruikt worden, met derden gedeeld worden, of als deze gelekt zijn. Leg procedures hiervoor van te voren vast. Maak waarschuwingen kort maar informatief. Waarschuw niet te vaak. Geef gebruikers de mogelijkheid in te stellen welke waarschuwingen ze willen ontvangen.

Informeren van gebruikers over de verwerking van hun persoonsgegevens (door een privacyverklaring) veronderstelt dat er een privacybeleid is (zie de 'Dwing af' strategie) waarop die verwerking gebaseerd is. Daarnaast moet volledige, up-to-date, informatie over de verwerking (wat, waar, wanneer) beschikbaar zijn. Dat laatste lijkt eenvoudiger dan het is.

> *Een aantal jaren geleden deden we een klein experiment met een aantal studenten om het recht op inzage te testen. De resultaten waren verbazingwekkend. We kregen letterlijk screenshots van databestanden. En één student werd gebeld door de help desk van zijn mobiele telefoon maatschappij. De arme helpdesk medewerker wou weten of hij zijn inzage verzoek echt door wou zetten, want het zou hem uren, zo niet dagen, kosten om alle informatie te verzamelen. Dat is de consequentie als je een systeem ontwerpt zonder rekening te houden met dergelijke inzageverzoeken.*

7.2 Voorbeelden

De Creative Commons pictogrammen worden gebruikt voor het samenvatten van het auteursrecht dat rust op een bepaald online document. Op een zelfde manier kunnen privacy pictogrammen de belangrijkste aspecten van een privacybeleid in één oogopslag zichtbaar maken. Bijvoorbeeld door met een aantal icons aan te geven welke soort gegevens worden verwerkt, waar deze verwerkt worden, en of ze met derden gedeeld worden (en zo ja, met wie).

Een persoonlijk privacy dashboard laat zien welke gegevens over gebruikers beschikbaar zijn, hoe ze verwerkt worden: waar ze voor gebruikt zijn, met wie ze gedeeld zijn, wanneer, hoe vaak. Bedrijven als Google hebben dergelijke dashboards ingericht. Zorg dat de toegang tot dit dashboard goed beveiligd is!

Apple's iOS laat in de statusbalk zien wanneer een applicatie gebruik maakt van locatiegegevens. Dit een voorbeeld van een 'ambient notification': de gebruiker wordt op een subtiele, niet invasieve, manier geïnformeerd over het gebruik van zijn persoonlijke gegevens.

8 Geef controle

Geef gebruikers controle over de verwerking van hun persoonsgegevens.

Controle is een fundamenteel principe om de privacy van gebruikers te beschermen. Privacy heeft niet als hoofddoel het delen en gebruiken van persoonlijke gegevens onmogelijk maken. Juist verre van dat! Maar dan wil je als gebruiker wel controle en zeggenschap hebben over de persoonsgegevens die verwerkt worden.

8.1 Tactieken

Gebruiker krijgen controle over de verwerking van hun persoonsgegevens middels een van de volgende tactieken.

Vraag toestemming (consent) Vraag gebruikers toestemming voor de verwerking van hun persoonsgegevens. Informeer ze hierbij vooraf over welke gegevens worden verwerkt, hoe die worden verwerkt, en met welk doel ('informed consent', zie ook de informeer strategie). Toestemming moet ingetrokken kunnen worden.

Geef keuze (choose) Geef gebruikers een reële keuze over de verwerking van hun persoonsgegevens. Basisfunctionaliteit moet beschikbaar zijn zonder verwerking van persoonsgegevens. Bied een (betaald) alternatief aan.

Corrigeer (update) Geef gebruikers de mogelijkheid om persoonsgegevens te corrigeren. Het ligt voor de hand dit te combineren met de mogelijkheid die gegevens in te zien (via een privacy dashboard).

Verwijder (retract) Geef gebruikers de mogelijkheid om persoonsgegevens te (laten) verwijderen. Ook dit kan gedaan worden via een privacy dashboard.

Toestemming vragen is niet altijd noodzakelijk, bijvoorbeeld als er een gerechtvaardigd belang is voor de verwerking. Win hierover advies van een jurist in.

Het is niet altijd mogelijk dan wel noodzakelijk om gebruikers de mogelijkheid te geven hun gegevens te corrigeren of te (laten) verwijderen.

Sommige persoonsgegevens zijn simpelweg noodzakelijk. In medische dossiers is het ongewenst om patiënten het recht te geven medische aantekeningen te laten verwijderen.

8.2 Voorbeelden

In veel gevallen is de verwerking van persoonsgegevens gewoon toegestaan, bijvoorbeeld omdat ze strikt noodzakelijk zijn voor het uitvoeren van een contract (denk aan een postadres bij het plaatsen van een bestelling) of omdat er een juridische verplichting is (controle van identiteit door banken). In andere gevallen moet om toestemming gevraagd worden. Informeer gebruikers duidelijk over het doel. En geef gebruikers een echte keuze (zodat ze ook zonder toestemming te geven toegang krijgen, eventueel tot een deel van de totale functionaliteit). Zorg voor *opt-in* (geen verwerking zonder toestemming vooraf) in plaast van *opt-out* (verwerking vind standaard plaats, tenzij achteraf toestemming wordt ingetrokken): de standaard keuze is *geen* toestemming. Dus geen 'voor-gevinkte' checkbox voor aanmelden op een nieuwsbrief, bijvoorbeeld…

Websites moeten om toestemming vragen voordat ze cookies gebruiken. Veel van de 'accepteert u cookies' meldingen voldoen niet: ze geven geen reële keuze omdat bij niet accepteren van cookies de website niet bezocht kan worden. Een goede cookieverklaring geeft de keuze om cookies al dan niet te accepteren, en de mogelijkheid in te stellen welke cookies (bijvoorbeeld voor het opstellen van statistieken of voor het koppelen met sociale netwerken) al dan niet te accepteren.

Een radicaal andere benadering legt de controle over zijn persoonsgegevens volledig bij de gebruiker zelf. In plaats van als organisatie de gegevens van al je klanten te bewaren, vraag je de klant dat zelf, op zijn eigen device, te doen. Als je bepaalde gegevens nodig hebt, vraag je die aan de klant (via een gestandaardiseerd protocol; de klant hoeft niets op nieuw in te voeren). Dit wordt wel 'customer managed relations' genoemd, als tegenpool van 'customer relations management'.

9 Dwing af

Committeer je aan een privacy vriendelijke verwerking van persoonsgegevens, en dwing deze af.

Privacy moet niet alleen technisch maar ook in organisatorisch zin beschermd worden. Het moet onderdeel zijn van de bedrijfscultuur en uitgedragen worden door de top van de organisatie. Anders zal niemand zich ervoor verantwoordelijk voelen. Een duidelijk privacybeleid schetst hiervoor de kaders. De 'dwing af' strategie is intern, op de organisatie, gericht. De strategie zorgt er voor dat de extern geformuleerde privacyverklaring (zie de informeer strategie) ook intern afgedwongen wordt door een privacybeleid (privacy policy).

9.1 Tactieken

Privacy vriendelijke verwerking wordt afgedwongen door de volgende tactieken na te volgen.

Stel vast (create) Committeer je als organisatie aan privacy. Neem je verantwoordelijkheid. Stel een privacybeleid op. Stel resources beschikbaar om het beleid uit te voeren. Bepaal per verwerking het doel, en de (juridische) grondslag: is er een gerechtvaardigd belang of moet er om toestemming gevraagd worden? Wees duidelijk over het verdien model.

Dwing af (uphold) Dwing het beleid af met alle noodzakelijke technische en organisatorische maatregelen. Implementeer deze maatregelen. Beleg verantwoordelijkheden. Stel een opleidingsprogramma en awarenesscampagne op. Zorg dat derden (de zogenaamde 'verwerkers') ook aan de eisen voldoen.

Beheer (maintain) Omstandigheden veranderen. Controleer het privacybeleid, en de implementatie daarvan, regelmatig, en pas waar nodig aan. Stel vooraf eisen op, en toets hier aan.

Zorg ervoor dat het privacybeleid in lijn is met het bedrijfsplan en missie van de organisatie. Zorg er ook voor dat het privacybeleid consistent is met overige beleidsregels.

9.2 Voorbeelden

En mogelijkheid is om een privacy management systeem op te zetten in navolging van de plan-do-check-act cyclus uit de information security management standaard (ISO 27001). Dit zou geïntegreerd kunnen worden met de gegevensbeschermingseffectbeoordeling (data protection impact assessment, DPIA) die toch al uitgevoerd moet worden (en die verder besproken worden onder de 'toon aan' strategie).

Een andere mogelijke technische benadering is het gebruik van zogenaamde 'sticky policies' die aan een data item worden gehangen, bijvoorbeeld om aan te geven voor welk doel het data item is verzameld, of welke soort verwerkingen toegestaan zijn. Processen in de organisatie zijn dan zo ingericht dat voor elk data item de bijbehorende sticky policy automatisch gecontroleerd wordt.

Te denken valt ook aan technieken die 'ongewoon' gebruik van data registreert en eventueel de toegang tot de data blokkeert, bijvoorbeeld als één persoon ongebruikelijk veel data opvraagt, of als opvallend veel personen inzage in één bepaald data item (bijvoorbeeld het medisch dossier van een bekende Nederlander) inzien.

Aandacht moet ook gegeven worden aan de systeem ontwikkel processen binnen de organisatie. Volg de privacy by design filosofie, en neem privacy bescherming vanaf het begin mee. Daar helpt dit boek je bij! ;-) Als je niet zelf je systemen ontwikkelt kan de privacy by design benadering, en zeker het gebruik van de privacyontwerpstrategieën, helpen om het bestek voor aan te schaffen systemen op te stellen.

10 Toon aan

Toon aan dat je op een privacy vriendelijke wijze persoonsgegevens verwerkt.

Deze strategie geeft invulling aan de nieuwe eis dat organisaties *aantoonbaar* moeten voldoen aan privacy wetgeving. De 'toon aan' strategie is extern, op de toezichthouder (eventueel via de interne functionaris gegevensbescherming), gericht.

10.1 Tactieken

De volgende tactieken helpen organisaties aan te tonen dat ze voldoen aan de wet.

Leg vast (record) Documenteer alle (belangrijke) stappen die je neemt. Leg beslissingen vast, en motiveer deze. Verzamel logs (en kom in actie bij anomalieën)[1].

Audit (audit) Voer regelmatig audits uit op de verzamelde logs, maar ook meer in het algemeen op de manier van werken in de organisatie, en op de manier van verwerken van persoonsgegevens.

Rapporteer (report) Rapporteer de resultaten van de audits aan de toezichthouder, of bewaar deze voor latere inzage. Overleg, waar mogelijk, regelmatig met de toezichthouder.

Documenteer zo efficiënt en volledig mogelijk op welke wijze de organisatie persoonsgegevens beschermt. Doe dit op een voor de toezichthouder overzichtelijke en inzichtelijke manier. En controleer of de documentatie strookt met de werkelijkheid.

10.2 Voorbeelden

Een privacy impact assessment (PIA) bepaalt voor een nieuw product of nieuwe dienst wat de privacy risico's zijn, en hoe die geadresseerd moeten worden. Een PIA moet altijd uitgevoerd worden. Soms volstaat een

[1] Deze tactiek heette 'log' in eerder stukken.

kleine PIA. Als de privacy risico's groot zijn is een volledige PIA vereist. Een PIA moet om de zoveel tijd herhaald worden: interne dan wel externe omstandigheden kunnen in de loop van het jaar veranderd zijn. Het vastleggen van de uitkomsten en de op basis daarvan genomen beslissingen of maatregelen vormen een goed uitgangspunt voor de 'toon aan' strategie.

Een andere benadering is gecertificeerd te worden tegen een (internationaal) erkende standaard voor privacy bescherming (zoals TRUSTe of EuroPriSe). Ook is het mogelijk om een benchmark uit te laten voeren met andere organisaties die werkzaam zijn in dezelfde branche, om zo de privacy-volwassenheid van de organisatie verder te onderbouwen.

Het gebruik van formele methoden en gestructureerde ontwikkel omgevingen voor de ontwikkeling van nieuwe systemen is aan te bevelen.

11 Toepassen

Traditioneel is systeemontwikkeling een cyclisch proces. Hierin worden een aantal verschillende fasen doorlopen: conceptformulering, definitie, ontwerp, ontwikkeling[1], implementatie[2], gebruik, evaluatie, en ontmanteling (zie figuur 11.1). De privacyontwerpstrategieën zijn ontwikkeld omdat bestaande instrumenten (ontwerppatronen, privacy enhancing technologieën) zich met name richten op de ontwerp en ontwikkelfase. Terwijl juist in de eerste twee fasen (conceptformulering en definitie) belangrijke beslissingen genomen worden die de privacy significant kunnen verbeteren (of aan kunnen tasten).

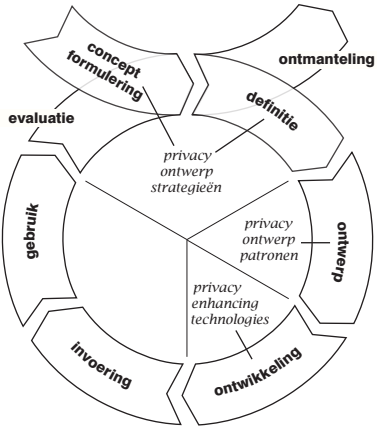
Het feit dat de privacyontwerpstrategieën zijn ontwikkeld in de context van een klassieke watervalontwikkelmethodiek betekent niet dat ze niet ook van toepassing zijn binnen modernere benaderingen, zoals agile softwareontwikkeling. Ook daar worden nieuwe concepten geformuleerd en gedefinieerd. De inpassing is alleen anders.

De privacyontwerpstrategieën stellen, vanuit een technisch perspectief, doelen die, als ze bereikt worden, de privacy van het systeem verbeteren. Je kunt ze ook zien als vragen die je jezelf kunt stellen tijdens het ontwikkelproces. Hoe kan ik de verwerking van persoonsgegevens scheiden? Hoe kan ik mijn gebruikers optimaal informeren over de verwerking van hun gegevens?

Dit kan op een redelijk gestructureerde manier gedaan worden. Zorg ervoor dat alle relevante partijen betrokken zijn bij het proces, zoals de proceseigenaar, en de inhoudelijk expert. Zorg er ook voor dat de eindgebruikers (wiens persoonlijk gegevens uiteindelijk zullen worden verwerkt) vertegenwoordigd zijn. Dit garandeert dat het proces (en dus de analyse van de risico's) niet alleen maar vanuit het perspectief van de verwerker doorlopen wordt.

De privacyontwerpstrategieën zijn niet alleen toepasbaar als je zelf systemen ontwikkelt. Ze kunnen ook gebruikt worden bij het opstellen van een pakket van eisen voor de aanschaf van een systeem.

[1] Inclusief testen en evaluatie.
[2] I.e. het invoeren in een organisatie of proces.



Figuur 11.1: Systeemlevenscyclus

Focus niet op één strategie. Het is niet zo dat je moet kiezen tussen strategieën. Ze zijn naast elkaar bruikbaar. Gebruik ze daarom allemaal om je systeem zo privacyvriendelijk mogelijk te maken. Wel is, afhankelijk van de context, de ene strategie belangrijker of beter toepasbaar dan de andere.

Bekijk alle vormen van verwerking van persoonsgegevens. Dat wil zeggen het verzamelen, opslaan, bewaren, gebruiken, verrijken, delen, veranderen en verwijderen van gegevens. Onderzoek voor iedere strategie (en taktiek) hoe die van toepassing zou kunnen zijn op elk van deze aspecten.

Beperk je niet tot het beschermen van 'gewone' persoonsgegevens, maar neem ook gedragsgegevens expliciet mee.

Tenslotte kun je overwegen om de strategieën per deelcomponent van je te ontwerpen systeem toe te passen. Dat kan zelfs recursief: een eerste ontwerp op basis van een analyse met privacyontwerpstrategieën kan verder verfijnd worden door de strategieën nogmaals toe te passen.

12 Ter afsluiting

De laatste versie van dit boek is te vinden op
http://www.deprivacycoach.nl.

De icons voor elk van de strategieën zijn beschikbaar in pdf en SVG formaat.

Wilt u op de hoogte blijven? Volg @deprivacycoach op Twitter, of abonneer je op de email lijst van http://www.deprivacycoach.nl.

Voor vragen op opmerkingen, email mij op info@deprivacycoach.nl. Ik hoor het graag als u de privacyontwerpstrategieën hebt gebruikt, en wat uw ervaringen daar mee waren!

En waarom heet dit "Het Blauwe Boekje"? Omdat blauw de kleur van vertrouwen is.

Mei 2018,
Jaap-Henk Hoepman.

12.1 Bronnen

- M. Colesky, J.-H. Hoepman, and C. Hillen. A Critical Analysis of Privacy Design Strategies. In 2016 International Workshop on Privacy Engineering (IWPE'16), pages 33-40, San Jose, CA, USA, May 26 2016.
- De Algemene Verordening Gegevensbescherming (AVG).
- G. Danezis et. al., Privacy and Data Protection by Design, ENISA Report, december 2014.
- De Privacy design patters databank (https://privacypatterns.org).

12.2 Instellingen

- De Autoriteit Persoonsgegevens (AP).
- De European Data Protection Board (EDPB) (voorheen de Article 29 Working Party).
- The European Data Protection Supervisor (EDPS).

- The Federal Trade Commission (FTC).
- Bits of Freedom of Privacy First.
- Het Privacy & Identity Lab (PI.lab).

12.3 Meer weten

- Jaap-Henk Hoepman and Marc van Lieshout: "Privacy". In E. R. Leukfeldt and W. P. Stol, editors, Cyber Safety: An Introduction, pages pp 75-87. Eleven International Publishing, The Hague, 2012.
- Dimitri Tokmetzis en Maurits Martijn, Je hebt wel iets te verbergen, De Correspondent, 2016.
- B. Schneier, "Data and Goliath", W. W. Norton & Company, 2016.
- De Privacy Wiki.

12.4 Commercieel gebruik

In de praktijk betekent dit dat ik een vergoeding verwacht voor bepaalde vormen van commercieel gebruik. Het idee is dat ik een eerlijke vergoeding ontvang voor de tijd en moeite die ik gestoken heb ik het schrijven van dit boek, naar rato van de *directe* inkomsten die jij ontvangt op basis van het gebruik van mijn werk.

Niet al het gebruik van dit werk in een commerciële context is beperkt. Het gebruik van dit boek voor het invoeren van een interne privacy by design benadering, of voor een interne training van medewerkers om het nivo van privacy bescherming te verhogen is toegestaan. In dit geval is mijn beloning dat jou producten en diensten privacy vriendelijker worden.

Echter, als je dit boek gebruikt als een significant onderdeel van een privacy by design training die je als commerciële dienst aan derden aanbiedt, of als je dit boek gebruikt als een significant onderdeel van een privacy by design methodologie die je commercieel bij derden toepast, dan creëert het gebruik van mijn werk *directe* inkomsten voor jou. Dit is in het bijzonder het geval als je (een link naar) mijn boek verspreid als onderdeel van het trainingsmateriaal. De omvang van de vergoeding hangt af van hoe significant mijn werk voor je is, en hoeveel omzet je op basis daarvan

realiseert. Omdat ik dat echter toch niet kan bepalen, ben ik simpelweg afhankelijk van je eerlijkheid om een passende inschatting te maken van hoeveel mijn werk jou waard is.

Neem voor meer informatie, of voor betaalopties, contact op met mij via info@deprivacycoach.nl.

13 Verklarende woordenlijst

Betrokkene Persoon wiens persoonlijke gegevens worden verwerkt. Vaak een (eind)gebruiker van een dienst of product.

Design pattern / ontwerppatroon Beschrijft een algemeen terugkerende structuur van onderling aan elkaar gerelateerde componenten, waarmee een generiek ontwerp probleem binnen een bepaalde context opgelost kan worden.

Persoonsgegeven Een gegeven dat direct of indirect herleidbaar is tot een (natuurlijk) persoon. Naam of burgerservicenummer zijn natuurlijk een persoonsgegeven. Maar een kenteken, of een IP adres ook. Dat maakt een gegeven al snel een persoonsgegeven.

Privacy by design Ontwerpfilosofie welk vereist dat privacybescherming vanaf het begin af aan meegenomen wordt bij het ontwerpen en bouwen van nieuwe systemen.

Toezichthouder De autoriteit die verantwoordelijk is voor het handhaven van de privacy wetten. In Nederland is dit de Autoriteit Persoonsgegevens.

Verantwoordelijke Partij die bepaalt welke persoonsgegevens worden verwerkt, hoe die worden verwerkt en met welk doel. In het algemeen die diensten of producten aan eindgebruikers aanbiedt.

Verwerken Het op enigerlei wijze verzamelen, opslaan, bewaren, gebruiken, verrijken, delen, veranderen en verwijderen (van gegevens).

Verwerker Partij die persoonsgegevens verwerkt in opdracht van de verantwoordelijke.

Hoe maak je privacy by design concreet? Hoe pas je het in de praktijk toe? Daar geeft dit boek antwoord op.

Dit boek is geschreven door Jaap-Henk Hoepman. Hij is privacy expert, verbonden aan de vakgroep informatica van de Radboud Universiteit en de rechtenfaculteit van de Rijksuniversiteit Groningen. Hij is principal scientist van het Privacy & Identity Lab.