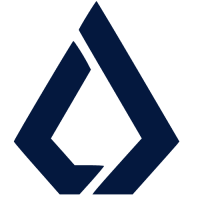
Case study: GDPR and Data Complexities

Seven step approach



Project: Lisk Delegates

Project team: BBB-BC

Team: Joeri Berman (2834499)

Luc Urlings (3071081)

Stijn Baltessen (3064565)

Wouter Vandenboorn (3099571)

Floris Feddema (3188256)

Davy de Haas (3099695)

Opdrachtgever: Study case, Bartosz

Versie: 0.1

Versie datum: 21 april 2020

Status: Concept

# Document revisies

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Wijzigen** | **Auteur** | **Datum** |
| 0.1 | Opzet Document | Stijn Baltessen | 21-04-2020 |

# Inhoudsopgave

[**Document revisies**](#_bu2l4jqkimrr) **2**

[**Inhoudsopgave**](#_nyq276qpg8em) **3**

[**Seven step approach**](#_djfvx4apkl6h) **4**

[**1. Bespreek de casus**](#_o18hst4mn4x8) **5**

[**2. Identificeer de vragen**](#_tjp21jqbwrox) **6**

[**3 + 4. Brainstorm & Analyseer**](#_drphanabweja) **7**

[**5. Formuleer de leerdoelen**](#_gbd35qg6f1fh) **8**

[**6. Individuele studie**](#_p83oa97dizn9) **9**

[Wat zijn de Hoofduitgangspunten van AVG?](#_6zfkgclg80mj) 10

[Hoe heeft de AVG betrekking op het hosten van software?](#_jvyoptvy70ec) 12

[Wat voor maatregelen kan je nemen om ervoor te zorgen dat gevoelige gegevens op je laptop niet te verkrijgen zijn?](#_3q7y2lbvczcr) 13

[Hoe kan de AVG toegepast worden op encrypted data?](#_4atx3xx4wnao) 14

[Wat zijn de verantwoordelijkheden van een privacy officer?](#_16vjyr59k3ur) 15

[Zijn er instanties waarbij je kan laten verifiëren of je voldoet aan de AVG?](#_rvcbdxvixjww) 16

[**7. Discussieer de bevindingen**](#_ac7fflek5znk) **17**

[**Conclusie**](#_h492bksdlh42) **18**

# Seven step approach

Hier staan de zeven stappen van de [seven step approach](https://portal.fhict.nl/Studentenplein/LMC/1920vj/Software%20engineering/Afstudeerfase/EnterpriseSoftware/CaseStudies/SevenStepsApproach.docx) methode die bij probleem gebaseerd leren voorkomt.

1. Bespreek de casus
2. Identificeer de vragen
3. Brainstorm over potentiële bekende oplossingen
4. Analyseer resultaat van brainstorm sessie
5. Formuleer de leerdoelen en wat er nog geleerd moet worden
6. Individuele studie om de kennis van 5 te kunnen vergaren
7. Discussieer de bevindingen van 6 en hoe dit 5 en 2 beantwoord

# 1. Bespreek de casus

De drie opgesomde scenario’s moeten een stappenplan krijgen over hoe AVG hier ter sprake komt en het mogelijk is om AVG toe te gaan passen.

Hieronder de scenario’s

* Er is een project gehost zowel on premise als in een derde partij cloud. Het maakt gebruik van een CRM (Customer Relations Management) systeem en een schaalbare gedistribueerde database.
* Een werknemer heeft zijn laptop verloren waarop gevoelige data staat. Bijvoorbeeld: toegang tot het project,de source code en toegang tot het bedrijfsnetwerk via een VPN.
* De backups van de database zijn volledig encrypted. Het probleem is dat wanneer je een gebruiker moet verwijderen, dit niet op de backups kan omdat het hier encrypted is. Door deze encryptie kan de AVG niet worden naleven.

Het is goed om na te denken wat wij zouden doen in de situatie van onze neef. Moeten we wel melden dat de laptop open heeft gestaan en iemand mogelijk toegang tot gevoelige data heeft of vinden we dat we dit gewoon kunnen proberen te verbergen en mogelijk op een stagiair kunnen afschuiven.

# 2. Identificeer de vragen

Wat zijn de hoofduitgangspunten van AVG?

Hoe heeft de AVG betrekking op het hosten van software?

Wat voor maatregelen kan je nemen om ervoor te zorgen dat gevoelige gegevens op je laptop niet te verkrijgen zijn? (stel dat die gestolen is).

Hoe kan de AVG toegepast worden op encrypted data?

Wat zijn de verantwoordelijkheden van een privacy officer?

Zijn er instanties waarbij je kan laten verifiëren of je voldoet aan de AVG?

# 3 + 4. Brainstorm & Analyseer

* Wat houdt **AVG** precies in?

Floris: Het is de nederlands implementatie van de GDPR wat de privacy wetgeving is van europa.

Wouter: Het is alleen de nederlands vertaling van GDPR  
*Verder onderzoek komt hierover*

**Algemene verordening gegevensbescherming.**

Het is een lijst van regels hoe bedrijven met privacy om moeten gaan.

* Wat zijn de hoofduitgangspunten van AVG?

richtlijnen met betrekking op privacy gevoelige data en gegevens van toepassing op burgers en bedrijven.

* Hoe heeft de AVG betrekking op het hosten van software?

Geen voorkennis.

* Wat voor maatregelen kan je nemen om ervoor te zorgen dat gevoelige gegevens op je laptop niet te verkrijgen zijn? (stel dat die gestolen is).

Schrijf encryptie (bitlocker). Wachtwoord op je laptop. Autolock. Single Sign On. Laptop niet uitlenen. Password manager per wachtwoord laten authenticeren. Active directory services.

* Hoe kan de AVG toegepast worden op encrypted data?

Geen voorkennis.

* Wat zijn de verantwoordelijkheden van een privacy officer?

Het waarborgen van de AVG implementatie binnen een bedrijf.  
*Verder onderzoek.*

* Zijn er instanties waarbij je kan laten verifiëren of je voldoet aan de AVG?

ISO certificaten, audit bedrijven.

# 5. Formuleer de leerdoelen

De student weet inhoudelijk wat de AVG inhoudt.

De student weet waar hij op moet letten tijdens het ontwerpen en implementeren van een applicatie om te voldoen aan de gdpr wetgeving

De student heeft zich ontwikkelt in het beantwoorden van ethische vraagstukken in betrekking met het AVG.

# 6. Individuele studie

Wat zijn de hoofduitgangspunten van AVG? - Joeri & Stijn

Hoe heeft de AVG betrekking op het hosten van software? - Joeri & Stijn

Wat voor maatregelen kan je nemen om ervoor te zorgen dat gevoelige gegevens op je laptop niet te verkrijgen zijn? (stel dat die gestolen is). - Floris & Davy

Hoe kan de AVG toegepast worden op encrypted data? - Floris & Davy

Wat zijn de verantwoordelijkheden van een privacy officer? - Luc & Wouter

Zijn er instanties waarbij je kan laten verifiëren of je voldoet aan de AVG?- Luc & Wouter

## Wat zijn de Hoofduitgangspunten van AVG?

De AVG gaat over het rechtmatig omgaan met persoonsgegevens. De belangrijkste bepalingen uit de AVG zijn als volgt samen te vatten:

* Persoonsgegevens mogen alleen worden verwerkt in overeenstemming met de wet. Voor de betrokkene (dat is degene van wie de persoonsgegevens verwerkt worden) moet het behoorlijk en transparant zijn hoe en waarom de persoonsgegevens verwerkt worden.
* Persoonsgegevens mogen alleen verzameld worden met een gerechtvaardigd doel. Dat doel moet welbepaald zijn en vooraf uitdrukkelijk zijn omschreven. Het doel waarvoor een organisatie de persoonsgegevens gaat verwerken moet verenigbaar zijn met het doel waarmee de persoonsgegevens zijn verzameld.
* Verwerkt een organisatie of persoon persoonsgegevens? Dan moet de persoon van wie de persoonsgegevens worden verwerkt in ieder geval op de hoogte zijn van de identiteit van de organisatie of persoon die deze persoonsgegevens verwerkt (de zogeheten verwerkingsverantwoordelijke) en van het doel van de gegevensverwerking.
* Als organisaties persoonsgegevens verwerken, dan moeten ze daarbij als uitgangspunt hanteren ‘zo min mogelijk’. Dat houdt o.a. in dat de verwerking van de gegevens moet passen bij het doel waarvoor ze worden verwerkt.
* De verwerkingsverantwoordelijke moet ervoor zorgen dat de gegevens juist zijn en zo nodig worden geactualiseerd.
* De gegevensverwerking moet op een passende manier worden beveiligd. Voor bijzondere gegevens, zoals over ras, gezondheid en geloofsovertuiging, gelden extra strenge regels.

|  |  |
| --- | --- |
|  |  |

Bron([Algemene verordening gegevensbescherming (AVG)](https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/algemene-verordening-gegevensbescherming-avg))

Bron([Checklist: houd grip op persoonsgegevens](https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/checklist_houd_grip_op_persoonsgegevens_def.pdf))

## 

## Hoe heeft de AVG betrekking op het hosten van software?

Dit heeft vooral betrekking op wanneer jou software dat gevoelige data opslaat, hoe en waar. En dat de gebruiker inzage in kan krijgen indien aangevraagd wordt.  
  
Als de data buiten de eu wordt opgeslagen kunnen hier andere regels op van toepassing zijn en de gebruiker moet hierover geïnformeerd worden.

Binnen de EU heeft een hosting bedrijf bepaalde standaarden, maar buiten de EU gelden er andere regelingen, als bedrijf ben je wel nog steeds aansprakelijk als er iets fout gaat als je hier je hosting hebt.

Gebruikers hebben het recht om zich vergeten te worden zonder onredelijk vertraging. (wissen of anonimiseren). Dus hier moet je software rekening houden.

Moet reactief kunnen zijn bij een datalek.

Als bedrijf ben je de afnemer van data ben je verantwoordelijk voor wat er met de data gebeurt en jij bent verantwoordelijk dat de data veilig wordt opgeslagen zelfs bij het gebruik van externe opslag.

Data moet niet toegankelijk zijn door 3de partijen zonder dat de gebruiker dit weet, gebruiker moet hiermee instemmen. Gebruiker moet het recht en de optie hebben om deze toestemming in te trekken.

## Wat voor maatregelen kan je nemen om ervoor te zorgen dat gevoelige gegevens op je laptop niet te verkrijgen zijn?

* Schijf encryptie - Het gebruiken van encryptie op een schijf maakt het mogelijk om data hierop te beveiligen. De schijf is dan ook alleen maar bruikbaar zodra je ook de sleutel hiervoor hebt. Dit zorgt ervoor dat als de schijf wordt gestolen de data niet toegankelijk is zolang de sleutel nog veilig is.
* Vergrendeling - Maak gebruik van een veilig wachtwoord, pin of een security key voor de vergrendeling van je apparaat.
* Autolock - Met autolock kun je je apparaat verbinden aan je telefoon met bluetooth. Zodra de bluetooth verbinding wordt verbroken zal het apparaat automatisch vergrendeld worden, als dat nog niet het geval is.
* SSO (Single Sign On) - Hiermee is het mogelijk om met één wachtwoord in te kunnen loggen. Dit zorgt ervoor dat er niet meerdere wachtwoorden moeten worden onthouden zodat het opschrijven op bijvoorbeeld een post it note wordt vermeden.
* Password manager - Maak gebruik van een password manager die per wachtwoord moet worden geauthenticeerd.
* Niks uitlenen - Zorg ervoor dat niemand anders zomaar op je apparaat kan zitten of het uitleent.
* LDAP (Lightweight Directory Access Protocol) - Dit protocol maakt gebruik van de X.500 standaard en wordt vaak samen gebruikt met SSO. Het zorgt ervoor dat gebruikers kunnen worden gevalideerd zodra hij of zij een bepaald iets willen doen binnen het netwerk, zoals het bekijken, aanpassen of verwijderen van bestanden of bepaalde opties aan of uit te kunnen zetten.

## Hoe kan de AVG toegepast worden op encrypted data?

Het is op dit moment niet goed mogelijk om hier het recht om vergeten te worden op een goede manier toe te passen. De franse autoriteit heeft geoordeeld dat het niet nodig is om het recht om vergeten te worden ook toe te passen in backups. Wel is het een goede stap om als bedrijf goed stil te staan hoe het bedrijf hier in de toekomst mee om kan gaan. Hierbij kan men denken aan bijvoorbeeld per gebruiker een apart bestand te gebruiken zodat deze eenvoudig te verwijderen zijn.

## 

## Wat zijn de verantwoordelijkheden van een privacy officer?

DPO = Digital privacy officer ← Wettelijk verplicht om aangesteld te worden door een bedrijf

* De DPO mag geen instructies krijgen over de uitoefening van zijn of haar taak.
* Ontslag of het opleggen van sancties naar aanleiding van de uitvoering van de taken van de DPO is niet toegestaan, alleen bij niet of slecht functioneren kunnen maatregelen tegen de DPO worden genomen.
* De DPO moet de middelen, tijd en toegang tot systemen hebben om zijn of haar taak goed uit te kunnen voeren.
* De DPO mag geen nevenfuncties bekleden die eventueel kunnen leiden tot belangenconflicten.

Privacy officer is een DPO die niet wettelijk verplicht aangesteld wordt een keuze van een bedrijf dus. Een bedrijf bepaald dan dus ook wat de taken van een po zijn. Een po kan ook als versterking dienen van een DPO zodat deze de werkdruk aan kan.

[Wat heeft mijn organisatie nodig, een DPO of een Privacy Officer? | Considerati | Partners for the Digital World](https://www.considerati.com/nl/kennisbank/wat-heeft-mijn-organisatie-nodig,-een-dpo-of-een-privacy-officer.html)

## 

## Zijn er instanties waarbij je kan laten verifiëren of je voldoet aan de AVG?

Ja die bestaan. Een aantal voorbeelden van bedrijven die dit doen zijn:

1. <https://www.isoprivacy.nl/#home>
2. <https://www.qbit.nl/>
3. <https://www.dbaudit.nl/>

Hier staat kort uitgelegd hoe zo een audit uitgevoerd zal worden:

* <https://www.dbaudit.nl/wp-content/uploads/2018/11/DBaudit-whitepaper-Privacy-Audit-Proof.pdf>

# 7. Discussieer de bevindingen

Ethiek van verantwoordelijk over AVG en dataprotectie is binnen de groep besproken.

# Conclusie

* Er is een project gehost zowel on premise als in een derde partij cloud. Het maakt gebruik van een CRM (Customer Relations Management) systeem en een schaalbare gedistribueerde database.

Zolang de gebruiker hiervan weet en dat hij verder geïnformeerd is van wat er met de data wordt gedaan, dan is dit niet een probleem.

* Een werknemer heeft zijn laptop verloren waarop gevoelige data staat. Bijvoorbeeld: toegang tot het project,de source code en toegang tot het bedrijfsnetwerk via een VPN.

Autoriteiten moeten hierover worden geïnformeerd.

* De backups van de database zijn volledig encrypted. Het probleem is dat wanneer je een gebruiker moet verwijderen, dit niet op de backups kan omdat het hier encrypted is. Door deze encryptie kan de AVG niet worden naleven.