

Europese General Data Protection Regulation vs. Software pakketten (SaaS) met gegevensverwerking: een praktische analyse

Onderzoeksvoorstel Bachelorproef

Frederic' Terryn¹

Samenvatting

Sinds mei 2018 is de General Data Protection Regulation aangenomen binnen de EU. Deze regelgeving is van toepassing voor iedereen die digitaal informatie verzamelt, en is gemaakt om gebruikersgegevens beter beheerbaar te maken en te beveiligen. Deze regelgeving is uiterst belangrijk in de moderne samenleving en nabije toekomst om ieders privacy te beschermen. Vaak is het in de praktijk uiterst moeilijk om bestaande software volledig aan te passen aan de nieuwe regelgeving. Deze paper zal een praktische analyse bevatten uitgevoerd op een bestaand software pakket. Er zal worden onderzocht, hoe gegevens in de loop der tijd verspreid worden, hoe dit allemaal kan bijgehouden en beperkt worden, en hoe er zo efficiënt mogelijk kan worden voldaan aan de nieuwe regelgeving. Vanuit dit praktijkonderzoek zal een overzicht van efficiënte en noodzakelijke oplossingen opgesteld worden voor software pakketten in het algemeen.

Sleutelwoorden

Gegevensbescherming in bestaande software. GDPR — Gegevensbescherming — SaaS.

Co-promotor

Gunter van de Velde²

Contact: ¹ frederic.terrinn.w3919@student.hogent.be; ² ;gunter.vandeveld@insites-consulting.com

Inhoudsopgave

- 1 **Introductie**
- 2 **State-of-the-art**
- 3 **Methodologie**
- 4 **Verwachte resultaten**
- 5 **Verwachte conclusies**

1. Introductie

De EU heeft de General Data Protection Regulation (GDPR) aangenomen. Deze regelgeving is in het leven geroepen om internetgebruikers een betere beveiliging van, en beheer over, persoonlijke gegevens te bieden. Vanaf mei 2018 moet elke organisatie kunnen aantonen welke gegevens verzameld worden, hoe ze deze gegevens gebruikt en hoe ze die beveiligt. (PORTAL2018) Daarnaast heeft elke gebruiker ten alle tijde het recht om vergeten te worden: een verwijdering van al zijn persoonlijke gegevens uit het systeem.

Deze regelgeving is van toepassing op iedereen die gegevens opvraagt en verzamelt van internetgebruikers binnen de Europese Unie. Binnen grote organisaties is er vaak voor nieuwe software een bedrijfsstatement voor de werknemers welke methodes gebruikt

worden en hoe wordt voldaan aan de GDPR. Voor bestaande software is het vaak veel moeilijker. In software pakketten die al jaren bestaan zijn gegevens vaak een eigen leven gaan leiden. Volgens de GDPR moeten je nu op al moment al deze gegevens overal en volledig kunnen verwijderen, kunnen aantonen wie op welk moment toegang heeft gekregen, enzovoort. Vaak zijn er al minimale aanpassingen gemaakt binnen bedrijven, en zijn de privacy verklaringen geüpdatet. Maar dat is lang niet voldoende. Een grote uitdaging is om te zoeken waar gegevens zich allemaal bevinden, en wanneer ze verwijderd moeten worden dit op elke plek te doen, doorheen de structuur van de software.

Aangezien deze regelgeving heel jong is, en van toepassing is op alle gegevens van elke Europese gebruiker, zijn er nog heel veel vragen onbeantwoord. In de moderne samenleving waar privacy beleid steeds belangrijker wordt, is het van essentieel belang dat bedrijven zo snel mogelijk volledig kunnen voldoen aan de GDPR en hiervoor efficiënte oplossingen ter beschikking hebben.

2. State-of-the-art

Zoals in de introductie beschreven is de GDPR een zeer actuele regelgeving. Het is echter niet volledig nieuw, maar een vernieuwing van een bestaande regelgeving. De vorige versie dateerde van 1995 en was door de realiteit compleet achterhaald.

Vanwege de jonge leeftijd zijn er nog geen uitgebreide studies geschreven die een compleet overzicht bieden van de beste oplossingen en die developers kunnen helpen om te beslissen hoe ze hun bestaande software moeten aanpassen. Daarnaast zal dit onderzoek eerst specifiek uitgevoerd worden op een software pakket binnen een bedrijf.

Wat wel ter beschikking is, is informatie in korte blogs en tutorials, waarvan de betrouwbaarheid niet kan gegarandeerd worden. Voorbeelden daarvan zijn als een persoon een volledig overzicht wil krijgen van wat wel en niet kan, en welke tools hiervoor best gebruikt kunnen worden, zal hij vaak een groot aantal verschillende bronnen moeten raadplegen. In vele gevallen spreken deze bronnen elkaar tegen of zijn er kleine onduidelijkheden, en de lezer zal telkens zelf de betrouwbaarheid moeten inschatten.

3. Methodologie

In deze paper zal onderzocht worden in hoeverre developers rekening moeten houden met de GDPR en hoe die op dit moment veelal wordt geïmplementeerd. Er zal aanvankelijk onderzoek gedaan worden naar enerzijds het software pakket. De weg die gegevens kunnen afleggen, wie er allemaal toegang tot heeft, hoe dit bijgehouden wordt enzovoort. Anderzijds zal de GDPR beter bekeken worden om na te gaan aan wat zeker moet voldaan worden, en op welke manieren. Hieruit zal geconcludeerd worden waar er aanpassingen moeten gebeuren zodat het aangeboden software pakket voldoet aan de regelgeving. Deze aanpassingen zullen uitgevoerd worden, en veralgemeend voor andere software pakketten waar mogelijk.

4. Verwachte resultaten

Na het onderzoeken van de software moet er een duidelijk overzicht zijn van wat er wanneer gebeurt met alle gegevens, en hoe dit best kan gecontroleerd worden. Als resultaat zullen er zowel concrete oplossingen volgen die uit te voeren zijn op de bestaande software, alsook algemene, duidelijke en structurele oplossingen voor andere software pakketten die zich willen aanpassen aan de GDPR.

5. Verwachte conclusies

Verwacht wordt dat in bestaande software pakketten het een heel moeilijke opgave is te vinden wat er doorheen de volledige levensduur allemaal met gegevens gebeurt. Wel moet het mogelijk zijn deze gegevens optimaal te beveiligen, en ervoor te zorgen dat de privacy van gebruikers in verhoogde mate kan gegarandeerd worden. Het is vooral belangrijk dat organisaties kunnen aantonen dat ze uitgebreide stappen hebben ondernomen om software aan te passen aan de GDPR, al wordt verwacht dat perfectie hierin een utopie zal blijven.