**General Data Protection Regulations speech door EY**

**Chingiz**

In heel het GDPR verhaal kan men twee partijen onderscheiden, nl: bedrijven en consumenten. Voor de bedrijven zijn volgende zes hoofdprincipes van toepassing, wanneer er sprake is van het opslag van (gevoelige) persoonlijke data:

1. Doel opstellen: welk doel wil ik bereiken met het verkrijgen van persoonlijke data en welke data heb ik daarvoor nodig
2. Doel bekend maken aan consumenten, door vb disclaimers
3. Alleen nodige gegevens verzamelen, niet meer dan je als bedijf nodig hebt om je doel te kunnen bereiken
4. Gegevens niet langer opslaan dan nodig
5. Zien dat de opgeslagen gegevens correct zijn, anders heeft het geen zien en kan het zelfs tot gevaarlijke situaties leiden.
6. Gegevens veilig opslaan, enkel toegankelijk voor geautoriseerd personeel: role based access control

Deze principes zijn dikwijls moeilijk toepasbaar wegens legacy data opslag bij veel bedrijven (diskettes, hard disks, ...)  
  
Bovendien wil de overheid zware boetes opleggen aan bedrijven die het slachtoffer zijn geworden van security breaches en dit verzwijgen. De boetes kunnen oplopen tot 4% van de totale omzet.  
  
Als consument krijg je bepaalde rechten, zoals:

1. Vragen om gegevens te wissen bij eender welk bedrijf dat je gegevens opslaat
2. Toestemming om data te verzamelen terug kunnen trekken
3. Recht om toegang te krijgen tot jouw gegevens en de wijze waarop ze verwerkt worden.
4. Vragen om jouw gegevens niet meer te verwerken
5. Klacht indienen bij privacy commissie als je meent dat jouw gegevens op een niet correcte manier opgeslagen en/of verwerkt worden.
6. Vragen om jouw gegevens door te sturen naar een ander bedrijf, op jouw vraag

Je als consument hebt dus altijd het recht om zelf te beslissen wie, wat en op welke manier jouw data mag opslaan en verwerken.

Er zijn 5 grote conclussies die we kunnen trekken, nl:

1. It, juristen en security specialisten moeten heel nauw samenwerken om te kunnen garanderen dat GDPR effectief toegepast wordt
2. Legacy: papier, andere dragere, niet up to date pcs en servers maken het extra moeilijk in GDPR toe te passen.
3. Nieuwe systemen die ontwikkeld worden moeten rekening houden met GDPR en dus extra middelen insteken om dit te bereiken
4. Men moet weten waar de gegevens bewaard worden om ze te kunnen verwerken en beveiligen. Dit is soms lastig met legacy opslagmiddelen (archieven, wat bevind zich waar) en de Cloud oplossingen.
5. Mentaliteit van de mensen moet ook veranderen, niet alleen binnen IT systemin, maar ook naar de Social Engineering toe.

Reflectie van Sanjy:

Ik vond de sessie wel interessant en belangrijk voor ons. Want we gaan later in IT sector werken en we moeten de data beheren. De General Data Protection Regulation (GDPR) is een reeks van regels om de persoonlijke gegevens van Europese burgers beter beheren en beveiligen. De wetgeving werd op het einde van vorig jaar goedgekeurd, en als bedrijven of data gebruikers moeten we vanaf 2018 kunnen aantonen welke persoonsgegevens dat we verzamelt, hoe gaan we data gebruiken en beveiligen. Dit regels geldig alle data in de EU ligt, niet in de cloud buiten de EU beheert.

We als bedrijf eigenaar of werknemer, moeten we die die regels stipt volgen om boeten te vermijden. In geval van een datalek niet op juiste manier, binnen bepaalde tijd niet wordt gemeld of de data niet correct wordt behandeld dan kunnen de boetes oplopen 2 tot 4 procent van de totale omzet met maximum 20 miljoen euro.

Reflectie Chingiz

Voor me persoonlijk is GDPR een verzinsel om het leven van mensen moeilijker te maken en om de staatskas te kunnen vullen door fikse boetes te geven.

Er worden namelijk tal van omwegen voorzien om GDPR (niet) / gedeeltelijk toe te passen, zoals het ‘publiek belang’. Een zeer ruim begrip...

Anderzijds is het toepassen van GDPR moelijk bij grote bedrijven (ziekenhuizen, overheidsinstanties, banken,...) bedrijven met grote data opslagen, die op legacy dragers staan.

Ik zou GDPR eerder als een richtlijn invoeren en elke bedrijf een optie geven in hoeverre ze deze richtlijn willen toepassen. Wel zou ik boetes voorzien als er dataleks zijn, maar dan los van het feit of GDPR toegepast werd of niet. Ik vind dat elke bedrijf zelf moet beslissen hoe ze met de data omgaan.