GDPR compliance voor zelfstandigen, KMO’s en grote ondernemingen

GDPR compliance voor zelfstandigen, KMO's en grote ondernemingen
Het privacyrecht vandaag

De Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens
Op basis van Richtlijn 95/46/EG - Boek XII WER

Andere tijden…

Geen online marketing
Geen "profiling"
Geen "cookies"
Geen "tracking"
Geen "location based marketing"
Geen "trigger based marketing"
Geen e-commerce
Geen social media
Minder dan 1% van de EU-bevolking gebruikte internet in 1995…

GDPR compliance voor zelfstandigen, KMO's en grote ondernemingen

Privacy compliance vanaf 25 mei 2018

In werking op 25 mei 2018
Géén overgangsperiode

Privacycommissie zal (zeer hoge) boetes kunnen opleggen

Elk bedrijf dat data in handen heeft moet zich in regel stellen
+ zal van zijn leveranciers, onderaannemers te… verwachten dat zij in regel zijn

Beursgenoteerde bedrijven, banken, financiële instellingen, gereguleerde sectoren nemen voortouw

GDPR compliance is onvermijdelijk

Bedrijven kunnen best GDPR compliance zien als asset ipv als risico of last…

GDPR compliance voor zelfstandigen, KMO's en grote ondernemingen

Privacy compliance raakt ELK bedrijf

GDPR compliance is onvermijdelijk voor elk bedrijf dat data verwerkt

De facto verwerkt ELK bedrijf beschermde persoonsgegevens:

HR afdeling houdt personeelsgegevens
Procurement houdt data over leveranciers
Sales en marketing houden data over klanten en prospects
Accounting houden gegevens over alle lagen van bedrijf heen

Al deze data bevat potentieel beschermde persoonsgegevens, waardoor GDPR compliance verplicht wordt

+ GDPR compliance wordt vereiste voor wie data van derden verwerkt, gebruikt of aanstuurt (reclamebureaus, softwareleveranciers, webplatformen, …)

GDPR compliance voor zelfstandigen, KMO’s en grote ondernemingen

Impact van GDPR op bedrijfsprocessen

Interne business processen

Werken met onderaannemers die data verwerken

Verplichting om enkel te werken met “veilige” onderaannemers (garanties vragen)
Verplichting om geschreven contracten te hebben
Lijst van verplichte clausules in zulke contracten

= Noodzaak tot audit of mapping van onderaannemers / service contracten

GDPR compliance voor zelfstandigen, KMO’s en grote ondernemingen

Impact van GDPR op bedrijfsprocessen

Interne business processen

Logboek van verwerkingsactiviteiten

Verplichting om een “logboek van verwerkingsactiviteiten” bij te houden
Daarin ID verwerker, verwerkte data, categorieën, transfers, time limits, veiligheidsmaatregels
In geschreven vorm op de zetel van de vennootschap

GDPR compliance voor zelfstandigen, KMO's en grote ondernemingen

Impact van GDPR op bedrijfsprocessen

Interne business processen

Data security maatregels

"*Processor shall implement* ***appropriate technical and organizational measures****, to ensure an appropriate level of security"*
Pseudonymisatie waar mogelijk, confidentialiteit, security, back ups, security testing protocols, …

= Noodzaak tot audit / mapping van data binnen bedrijf

GDPR compliance voor zelfstandigen, KMO's en grote ondernemingen

Impact van GDPR op bedrijfsprocessen

Interne business processen

Data Protection Impact Assessment

Als mogelijks grote impact op privacyrechten
Verplichting om voorafgaande impact assessment te houden
Advies van DPO vereist als er een DPO is
Moet als basis dienen voor security beleid
Privacycommissie moet nog specifiëren wanneer DPIA vereist is
Als DPIA hoog risico toont: voorafgaand advies van Privacycommissie vragen

GDPR compliance voor zelfstandigen, KMO's en grote ondernemingen

Impact van GDPR op bedrijfsprocessen

Interne business processen

Data breach notificatieplicht

Verplichting om Privacycommissie te verwittigen van elke data breach
Asap of ten laatste binnen 72 uur
Aard van de breach, mogelijke gevolgen, genomen maatregelen, etc… (= verplichting om data breach te documenteren)
= plicht om data breach procedure in place te hebben

Als er mogelijke ernstige gevolgen zijn voor privacy van data subjects: plicht om hen in persoon te verwittigen!

GDPR compliance voor zelfstandigen, KMO's en grote ondernemingen

Impact van GDPR op bedrijfsprocessen

Interne business processen

Data Protection Officer

Als kernactiviteit bestaat uit verwerken van persoonsgegevens
Of data monitoring op grote schaal vereist
Of bestaat uit data monitoring op grote schaal

Voorwaarden en vereisten nog to be implemented

Informeren & adviseren, monitoren van compliance, SPOC voor authoriteiten

GDPR compliance voor zelfstandigen, KMO's en grote ondernemingen

Impact van GDPR op database management

Informatieplichten en toestemming

Wettigheid van verwerking ("op welke gronden mag ik data verwerken?")

Voorafgaande opt-in blijft de basisregel (+ vanaf nu bewijs vereist!)
"Verwerking is noodzakelijk om contract uit te voeren"

"Gerechtvaardigde redenen"
DM "***may*** *be considered*" een rechtvaardige reden, maar "*Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means*"
Dus: als bestaande klantenrelatie: OK, anders niet zomaar automatisch OK

GDPR compliance voor zelfstandigen, KMO's en grote ondernemingen

Impact van GDPR op database management

"Voorwaarden voor toestemming"

Verantwoordelijke moet kunnen bewijzen dat hij toestemming heeft (was al impliciet zo)
Verzoek om toestemming moet in begrijpelijke, duidelijke en eenvoudige taal gevraagd en onderscheiden van andere gevraagde akkoorden
Betrokkene kan toestemming op elk ogenblik intrekken (geen terugwerkende kracht)

Toestemming moet vrij gegeven zijn: géén toestemming verplichten voor verwerking die niet noodzakelijk is voor leveren van dienst/uitvoeren van overeenkomst
Klassiek voorbeeld: verplichte opt-in om korting te krijgen of om aan wedstrijd deel te nemen
(is in aantal lidstaten nu al verboden)

GDPR compliance voor zelfstandigen, KMO's en grote ondernemingen

Impact van GDPR op database management

Informatieplichten en toestemming

Verwerking van gegevens van een minderjarige (-13 jaar, -16 jaar)

Altijd expliciete toestemming van ouders vereist!

"redelijke inspanningen" om leeftijd te checken en toestemming te bekomen

eID?, Facebook login?, credit card data?, live chat, …?

GDPR compliance voor zelfstandigen, KMO's en grote ondernemingen

Impact van GDPR op database management

Informatieplichten en toestemming

Verplichting om betrokken te verwittigen als zijn gegevens verzameld of doorgegeven zijn zonder zijn voorafgaande toestemming

Binnen 30 dagen of bij eerste contact

= Data bekomen van data brokers, partner organisaties, online verzameld…

Verplichting vervalt als

Betrokkene al op de hoogte is of informatieplicht disproportionele inspanning vereist (= open door voor creativiteit…)

GDPR compliance voor zelfstandigen, KMO's en grote ondernemingen

Impact van GDPR op database management

Profiling & Electronic Decision Making

Profilering: *"**elke** vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een **natuurlijke persoon worden geëvalueerd**, met name met de bedoeling zijn beroepsprestaties, **economische situatie**, gezondheid, **persoonlijke voorkeuren, interesses, betrouwbaarheid**, gedrag, **locatie** of verplaatsingen te analyseren of te voorspellen;"*

Véél ruimer dan oude definitie. Vroeger enkel als volledig geautomatiseerd en als er gevolgen voor de persoon aan verbonden waren.

GDPR compliance voor zelfstandigen, KMO's en grote ondernemingen

Impact van GDPR op database management

Informatieplichten en toestemming

Recht om zich te verzetten tegen Profiling & Automatic Decision Making

Recht
Niet onderworpen te worden aan automatische beslissingen (of profiling) – Excepties (bvb contracten)
Die juridische gevolgen of andere significante gevolgen hebben
Die enkel gebaseerd zijn op automated processing of data
Die bedoeld zijn om persoonlijke kenmerken te analyseren

Voorbeelden
Prestaties op het werk, kredietwaardigheid en betrouwbaarheid
Geldt ook voor DM "beslissingen" (bvb send offer of niet)

GDPR compliance voor zelfstandigen, KMO's en grote ondernemingen

Impact van GDPR op database management

En nog veel meer…

Right to be forgotten

Pseudonieme data

"Data portability"

"Privacy by design"

"privacy by default" (cfr. recent Telenet "personalized advertising…")

…

GDPR compliance voor zelfstandigen, KMO's en grote ondernemingen

GDPR compliance traject

Be prepared…

Belangrijkste artikels (cfr. profiling = high risk processing)
Boetes tot 20 mio euro
Boetes tot 4% van wereldwijde omzet

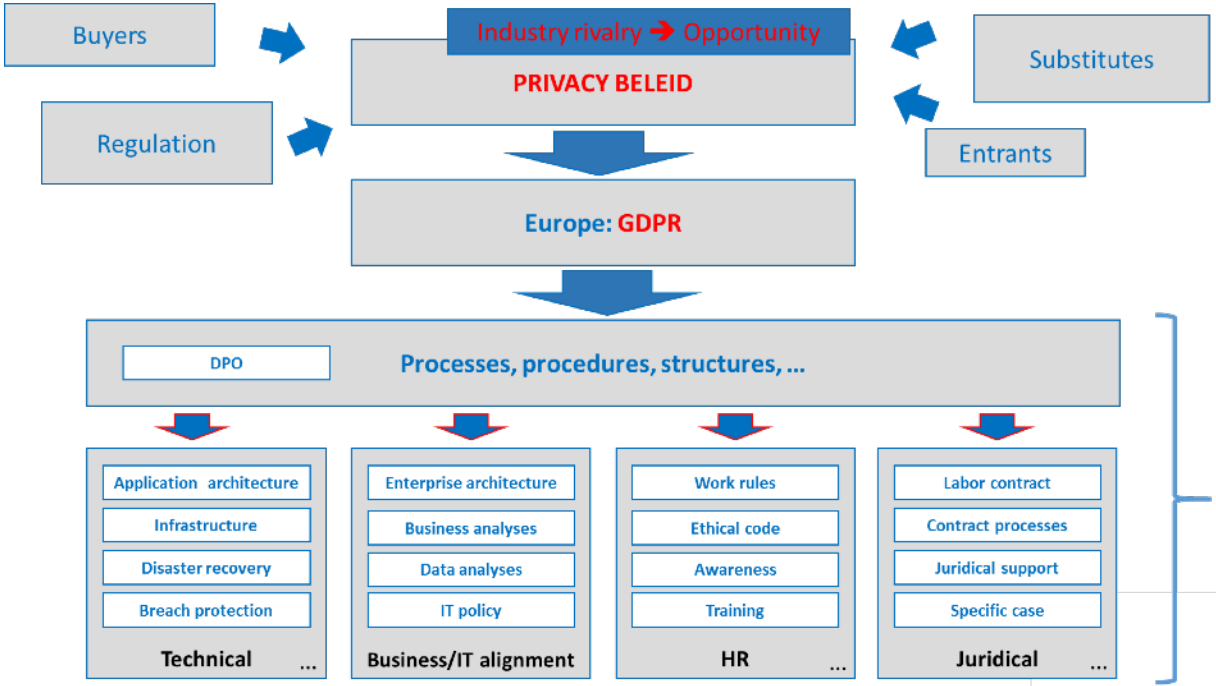
Hervorming van Privacycommissie zal leiden tot effectieve controles
Level playing field in EU zal leiden tot (strenge) controles op niveau van buurlanden

+ schadevergoeding voor betrokkenen

GDPR is niet alleen risico, maar opportuniteit (compliancy als sales argument)

GDPR compliance voor zelfstandigen, KMO's en grote ondernemingen

GDPR compliance traject

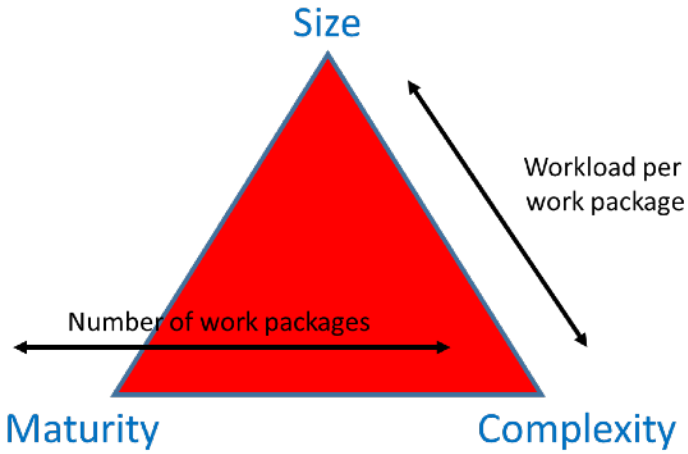


SIRIUS.LEGAL
BUSINESS LAW FIRM

GDPR compliance voor zelfstandigen, KMO's en grote ondernemingen

Work load van GDPR compliance traject

- Depends from company tot company

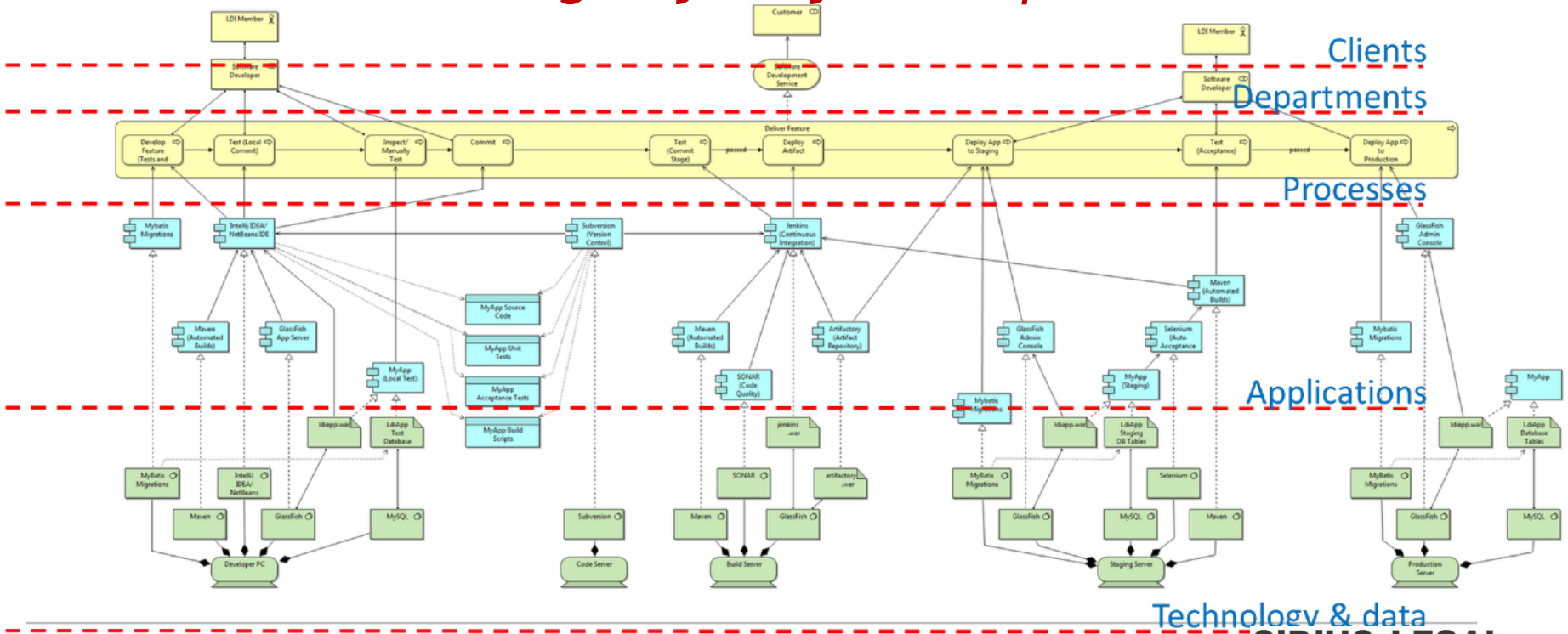


+ Internal workload!

SIRIUS.LEGAL
BUSINESS LAW FIRM

GDPR compliance voor zelfstandigen, KMO's en grote ondernemingen

"Baseline" nulmeting en jaarlijks actieplan

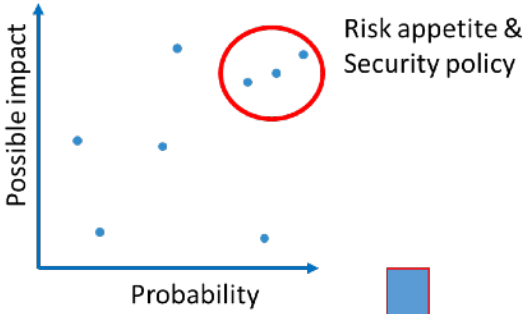


SIRIUS.LEGAL
BUSINESS LAW FIRM

GDPR compliance voor zelfstandigen, KMO's en grote ondernemingen

"Baseline" nulmeting en actieplan

Baseline:
- Identification of processes, data, systems
- Identification of risks



Yearly action plan

SIRIUS.LEGAL
BUSINESS LAW FIRM

GDPR compliance voor zelfstandigen, KMO's en grote ondernemingen

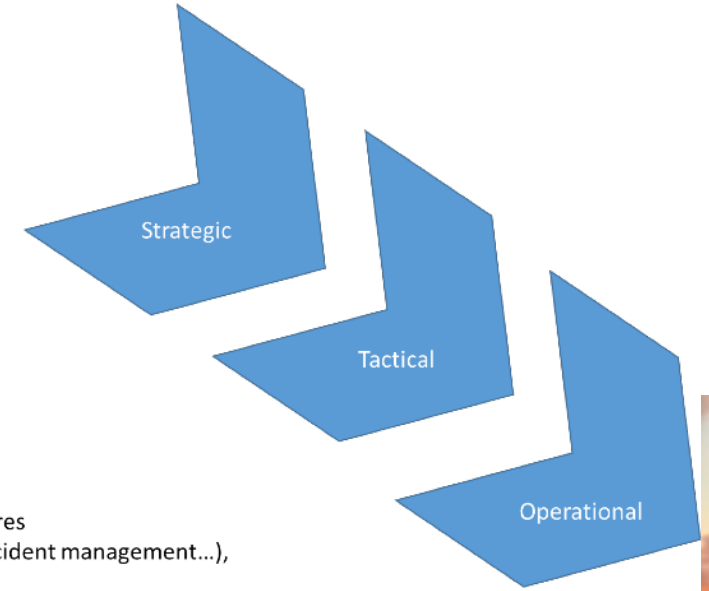
GDPR actieplan

Privacy policy

Baseline & risk analyses

Yearly action plan

Bring live procedures & structures
(Steering committee, PMO, Service delivery, PIA, Incident management…),
Create awareness.



SIRIUS.LEGAL
BUSINESS LAW FIRM

GDPR compliance voor zelfstandigen, KMO's en grote ondernemingen

GDPR compliance traject i.s.m. Sirius Legal

Gespecialiseerd en ervaren advocatenkantoor I.s.m. bekwame IT specialisten VUB/iMinds

Vrijblijvende intakegesprek met eerste analyse

Offerte op maat voor uw bedrijf op basis van 4 pijlers (Legal, HR, IT en Business processen)

SIRIUS.LEGAL
BUSINESS LAW FIRM

GDPR compliance voor zelfstandigen, KMO's en grote ondernemingen

Timing en work load GDPR compliance traject

Zelfstandigen
Work load +/- 2 dagen
Timing traject: 3 à 4 weken

KMO's
Work load
ifv omvang, maturiteit en complexiteit
tussen 5 en 25 dagen
Timing traject: 1 à 4 maanden

Grote ondernemingen
Work load ifv omvang, maturiteit en complexiteit
tussen 15 en … dagen
Timing traject: 2 à 6 maanden

GDPR compliance voor zelfstandigen, KMO's en grote ondernemingen

Aanzet package deal kleine ondernemingen

Bronze Compliance Package	Silver Compliance Package	Gold Compliance Package
Ons aanbod voor zelfstandigen, kleine ondernemingen of ondernemingen die slechts in zeer beperkte mate met persoonsgegevens in aanraking komen	*Voor KMO's en voor zelfstandigen of kleine bedrijven die op grotere schaal met persoonsgegevens werken (bvb de meeste webshops)*	*Voor grote ondernemingen en elke onderneming of organisatie die op grote schaal data verwerkt (reclamebureaus, HR bedrijven, openbare besturen, scholen, vakorganisaties, grote webshops, retailketens, ...*
Informatiebrochure Privacy Impact Assessment Actieplan obv PIA Privacy en cookie policy Clausules leverancierscontracten Clausules arbeidsovereenkomsten Bring your own device policy Interne data protection policy 4 uur Individuele consultancy	Informatiebrochure Privacy Impact Assessment Actieplan obv PIA Privacy en cookie policy Clausules leverancierscontracten Clausules arbeidsovereenkomsten en/of arbeidsreglement Bring your own device policy Interne data protection policy 15 uur Individuele consultancy + Bijstand op IT en business process vlak via onze externe partners 4 uur interne opleiding	Informatiebrochure Privacy Impact Assessment Actieplan obv PIA Privacy en cookie policy Clausules leverancierscontracten Clausules arbeidsovereenkomsten en/of arbeidsreglement Bring your own device policy Interne data protection policy Individuele consultancy op maat Bijstand op IT en business process vlak via onze externe partners + Follow up en bijstand gedurende 1 jaar 8 uur interne opleiding Data export clausules ...
€ 2.500,00 excl. BTW	**Ifv complexiteit onderneming tussen € 5.000,00 en € 10.000,00**	**Offerte op maat op basis van vrijblijvend intakegesprek**

SIRIUS.LEGAL
BUSINESS LAW FIRM

SIRIUS.LEGAL

BUSINESS LAW FIRM

Ons IT/IP/Media team

Media & advertisement law
Copyright - trademarks - databases - software - knowhow
Travel & consumer protection
IT, Internet & e-commerce
Privacy & cookies
Gambling & gaming

Contacteer ons vandaag nog
info@siriuslegal.be
www.siruslegal.be
Facebook.com/siriuslegal

SIRIUS.LEGAL

BUSINESS LAW FIRM