WEBINAR

Global Data Privacy Laws - Ripple Effect of GDPR

Sheila M. FitzPatrick

WORLDWIDE GDPR CHIEF PRIVACY OFFICER, DATA PRIVACY & SOVEREIGNTY LAWS

Gert Beeckmans

CHIEF RISK AND SECURITY OFFICER, SD WORX

Ascender sdworx

Our Speakers

Sheila FitzPatrick is considered one of the world's leading experts in data privacy laws, including the EU GDPR, and works closely with the US Government, Council of the European Union, country-specific data protection authorities in Europe, Asia/Pacific, and The Americas. Throughout her career, she holds strategic seats on several committees including the European Union Data Protection Advisory Council, the Asia Pacific Data Protection Framework Advisory Board and the Pacific Rim Privacy and Cybersecurity Advisory Group.

As the liaison between management and the Works Councils, She has written over 150 model contracts and bargaining agreements in over 60 countries, and achieved Binding Corporate Rules (BCRs) approvals for six multinational companies. Sheila provides expertise in global data protection compliance in over 160 countries, including the EU General Data Protection Regulation (GDPR), data sovereignty, cyber security regulations and obligations, legal issues associated with cloud computing and big data, data breach compliance and management, and records management. In the past 30 years she has helped over 200 multinational corporations achieve full worldwide data protection compliance approvals.
She has been recognised by Data Protection Authorities (DPAs) around the world for her in depth knowledge of comprehension and commitment to data protection laws.

Sheila was honoured as one of Silicon Valley's Women of Influence for 2017 and was also honoured as one of the 2017 EMEA 50, awarded to the 50 most influential people in Europe, the Middle East and Africa.

Gert Beeckmans
Chief Risk & Security Officer at SD Worx
Gert has led the Risk & Security team since January 2015, providing advice and guidance on information security and data privacy to all business units in the SD Worx Group. Gert is also responsible for the enterprise-wide security and data privacy programs for protecting customer information and personal data.

Since the beginning of his professional career, Gert has always had a passion and focus on security and privacy topics. He enjoys taking a risk-based approach in translating business requirements into concrete and pragmatic technical and organisational measures. Gert previously worked at the security and privacy team of Deloitte Enterprise Risk Services before joining SD Worx as IT Security Officer in 2008, and has been instrumental in building the information security within SD Worx group. In 2015, Gert was promoted to Chief Risk & Security Officer for SD Worx Group and his function was expanded to include data privacy and business continuity.

Ascender sdworx

Agenda

- Why the Expansion in Data Privacy/Protection Laws
- EU General Data Protection Regulation (GDPR)
- Role of Tools and Technology
- Ripple Effect of GDPR
- Risk Mitigation
- How GDPR affects HR operations in non-EU based companies
- Some practical real life HR cases
- Payroll Services Alliance: a common GDPR compliant approach
- Key Takeaways

Ascender sdworx

Why are Data Privacy Laws Expanding ?... Because...

- New technology driving the need for greater privacy rights (Cloud, IoT, AI)
- Prominent companies infringing on privacy rights
- Heightened concerns by individuals over the collection and use of personal data
- Lack of trust and transparency
- New business models – global expansion
- Intense media and social media focus on data privacy violations and security breaches (67% increase in 2017, 72% increase in 2018 already)
- Massive amount of data collected every day by unknown sources

As a result...

The biggest change in data privacy/protection laws in 25 years...

GDPR – New Gold Standard

- 11 chapters and 99 articles
- Addresses digital age
- Expanded data subject rights
- Differences in controller and processor responsibilities
- Mandatory reporting requirements
- Interaction with data protection authorities
- Stronger enforcement actions
- Transparency and trust
- Simplified terms of service agreements
- Policies must adhere to the laws

Webinar Progress

Ascender sdworx

GDPR Highlights

- First and foremost a **compliance** issue
- Impacts any company **regardless of location**
- Greater **data processor obligations**/accountability
- Data minimization
- Establishes EU Data Protection Board
- **Greater sanctions** – 4% of global annual revenue
- **Expands scope** of personal data
- **Lawful basis** for processing
- 72-hour data **breach notification obligations**
- **Privacy by Design**
- **Documentation** – clear and transparent policies and procedures
- Use of **Privacy Impact Assessments** (PIAs)
- **Appointment of Data Privacy Officer** (DPO) – internal or external
- **Right to be Forgotten**/Right of Erasure

Ascender sdworx

Definition of Personal Data

Personal Data	Any piece of information that is identifiable to a natural person or can identify a natural person either directly or indirectly. Includes business contact data, IP addresses, location data, biometric data, genetic information, unique identifiers
Sensitive Personal Data	Personal data revealing racial or ethnic origin, political affiliation, religious or philosophical beliefs, trade union membership, health or medical details, sexual orientation, criminal convictions
Non-personal data	Aggregate, statistical, or anonymous data that cannot be directly or indirectly tied back to a specific person in any way.
Data related to a company	May be confidential or restricted but is not considered personal data unless a person's information is included with the exception of some countries that consider data of legal entities personal data (e.g. China, New Zealand, Mexico, Russia, Taiwan)

Basis for Lawful Processing

- **Consent** – explicit and freely given (not appropriate in the context of employment)
- **Contractual necessity** – data subject is a party in the contract
- **Compliance with a legal obligation** - mandated by law
- **Vital interest of the data subject** – life or death situation
- **Public interest** – national safety
- **Legitimate interest** – cannot infringe on the rights of the data subject

Sanctions for Non-Compliance?

- Substantial fines for organizations that do not comply with the GDPR.
- Penalties of ten million euros or two per cent of global gross turnover (whichever is higher) for violations of record-keeping, security, breach notification and privacy impact assessment obligations.
- Doubled to twenty million euros or four per cent of global turnover for violations related to legal justification for processing violations, lack of consent, abuse of data subject rights and cross-border data transfers.
- Reputational damage
- Loss of contracts
- Restrictions on websites in countries

Webinar Progress

Tools and Technology Alone Do Not Solve GDPR

99 Articles in the GDPR – only 8 specifically involve tools and technology

Webinar Progress

GDPR Foundational Work is Essential

Start with the compliance foundation – don't start with the second floor

Webinar Progress

Data Privacy Versus Data Security

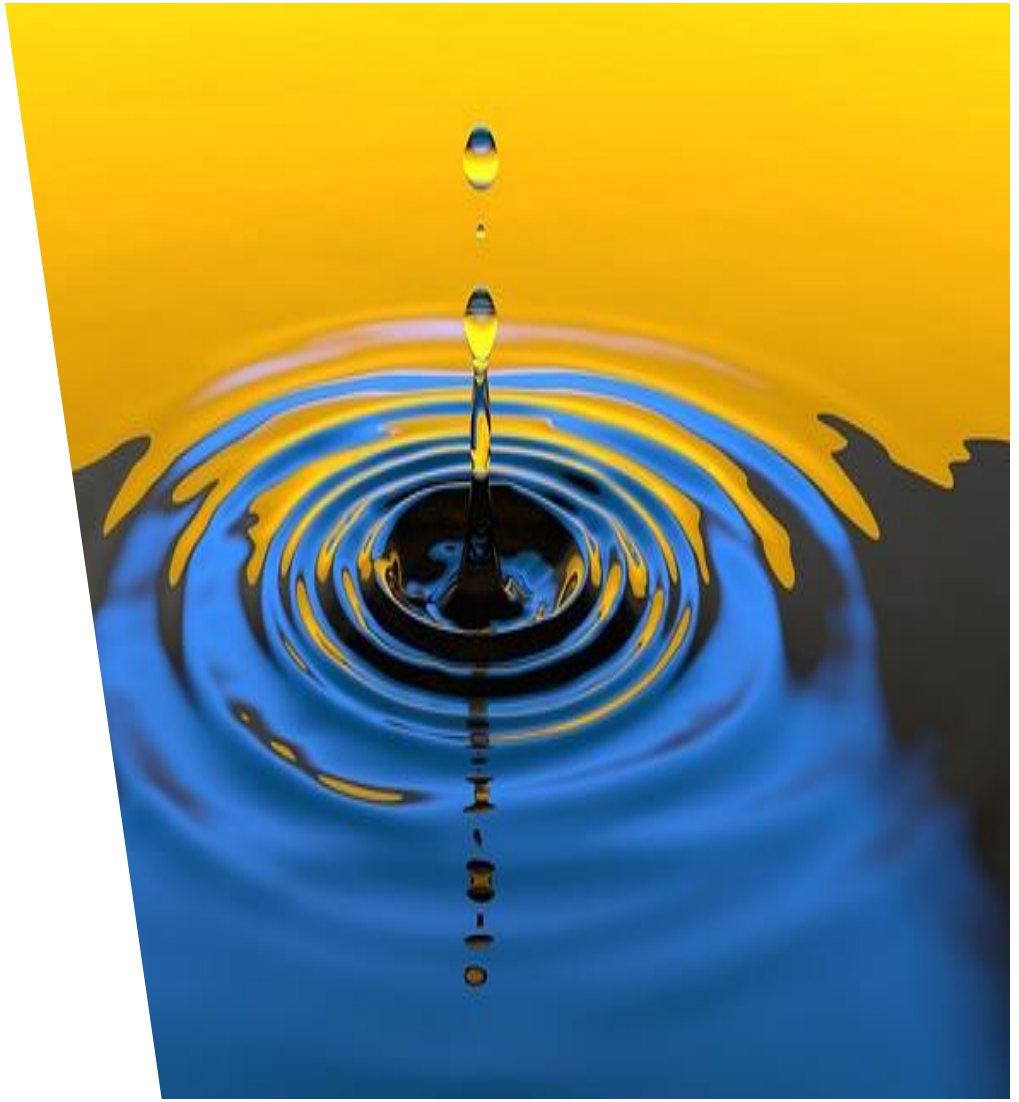
- Data security is NOT data privacy
- Privacy – legal collection, use, sharing , storage & transfer of data; legs & regs
- Security – fortress around the data
- Companies can have world class security, but no data privacy
- ISO standards and certifications address security not data privacy
- All cloud vendors can address security – few can address privacy
- Legal Privacy Impact Assessment - critical decision mechanism

Webinar Progress

Ascender sdworx

Ripple Effect of GDPR

- Awakening a global recognition of the importance of fundamental right to privacy
- Influx of marketing collateral, webinars, workshops – overwhelming and confusing
- So called “experts” jumped on the GDPR bandwagon
- Scaremongering – companies selling tools and technology to solve a legal issue
- No recognition of the importance of a solid data privacy compliance framework
- New need for Data Protection Officers (DPOs) - rare expertise
- Influencing change in other country-specific data protection laws



Country-Specific Legislative Impacts

ANZ

- Region trying to attract global business
- NSW - PPIP Act, HRIP Act, DPPs
- Australia – Amended Privacy Act – mandatory breach notification
- Australian Government Agencies Privacy Code (July 2018)
- New Zealand – “Adequacy” rating in question – enhancements coming

EMEA

- ePrivacy Act
- NIS Directive
- EU national laws
- DPAs – enforcement handled differently
- BREXIT
- Switzerland – assessing adequacy status
- Qatari, Saudi and UAE – most impacted
- Israel – Protection of Privacy Regulations and Protection of Privacy Law
- Data localisation

ASIA

- China – Cybersecurity Law – data localisation
- Japan – APPI mirrors GDPR – achieved adequacy rating
- Hong Kong – reforms parallel GDPR
- Philippines – Enhanced Rules & Regulations (IRRs) – align with GDPR
- Singapore – PDPA - sanctions (S$1M)
- South Korea – Personal Information Protection Act

THE AMERICAS

- USA – CLOUD Act, CA Consumer Privacy Act
- Canada - partial adequacy in question
- Brazil – Decree on Personal Data
- Chile – Personal Data Protection Act (PDPL)
- Colombia – Law 1581
- Costa Rica – Protection in the Handling of Personal Data of Individuals
- Mexico – Federal Law on the Protection of Personal Data

Ascender sdworx

GDPR Compared to Other Country-Specific Laws

Similarities:

- Consent obligations
- Privacy by design
- Compliance with privacy principles and obligations
- Transparency
- Data breach requirements
- Appointment of a Data Protection Officer
- Access to and correction of personal data
- Right to be forgotten
- Responsibility for 3rd party suppliers

GDPR Compared to Other Country-Specific Laws

Differences:

- Extraterritorial
- Includes the processing of all personal data, including employee
- Shorter time frame to report breaches
- Opt-out of automated processing
- Well defined privacy notices
- Expanded rights of data subjects
- Applies to both public and private sector
- Restrictions on overseas transfers
- More aggressive enforcement and greater sanctions

Risk Mitigation

- Be transparent
- Build the privacy foundation
- Understand what data is needed to run the business
- Identify what data is collected, processed, accessed, stored, transferred, etc.
- Minimize data collected
- Identify location and flow of data
- Vet third party providers and partners for privacy/GDPR compliance
- Take privacy compliance seriously (we take security seriously – why not privacy?)
- Don’t allow waivers that override privacy obligations
- Technology can’t drive privacy decisions – privacy should drive technology decisions
- Evolution not a revolution

Ascender sdworx

How GDPR affects HR operations in non-EU based companies

Ascender sdworx

Power to the individual: your EU employees have extensive rights on the personal data that you hold

1. Transparent information
2. Right of access
3. Right of correction
4. Right to erasure
5. Right to restrict processing
6. Right of data portability
7. Right to object to processing
8. Right to prevent use for direct marketing
9. Right to prevent use for scientific, historical or statistical purposes
10. Right to prevent automatic decisions
11. Right to compensation

Ascender sdworx

And you will have to be able to deal with these and answer these

- Informing employees on their rights
- Evaluating requests of employees in balance with your own obligations
- Respond within due time (30 days)

- Need for an adequate process and expertise/knowledge to answer such requests within an HR context

Use HR software and trusted partners that know what it’s all about and that allow you to answer these requests in a streamlined way

Ascender sdworx

Some practical real life HR cases

Ascender sdworx

Example 1: HR service center outside EU

We have HR service center in Singapore delivering also services to all our EMEA employees.

Which controls should we minimally take to ensure GDPR compliance?

Ascender sdworx

Example 1: HR service center outside EU

- You should transparently communicate to your EU employees on which HR data is processed by your Singapore HR service center. This can be done through an HR privacy notice/statement, clauses in the employment contract, etc.
- You should ensure an appropriate legal transfer mechanism is in place between all your EU based entities and the service center in Singapore (e.g. data processing agreement based on the EU model clauses)
- Employees in your Singapore HR service center must be aware of the individual rights that your EU employees have. Make sure they understand them and that there is a clear process to record and answer any requests
- Review your data breach procedures that your Singapore HR service center applies for compliance and ensure these are strictly followed

Ascender sdworx

Example 2: Handling a data breach

Due to a processing error, your EU payroll provider has uploaded a number of employees with the same employee number. As a consequence, the generated pay slips contained information of multiple individuals, hereby giving access to pay slip information of a co-worker.

What should you do?

Ascender sdworx

Example 2: Handling a data breach

- Inform your Data Protection Officer or Privacy Officer to initiate your own privacy incident process
- If he is not aware yet, contact your payroll provider. Make sure the incident is contained and ensure that access to the pay slips is disabled immediately. Request a full impact assessment and incident report:
  - Which categories of personal data were breached?
  - Which individuals were affected?
  - What was the potential impact of the leak on the affected individuals?
  - What measures have been taken and are still planned?
- Assess yourself the risk on the rights and freedoms of the affected individuals and determine whether you must notify the data protection authority and/or the affected individuals within 72 hours

Example 3: Data subject rights

Mrs. X was dismissed and requests from her previous employer a copy of certain documents that contains her (processed) personal data e.g. e-mails, evaluation forms.

Example 3: Data subject rights

- Mrs X has a right to obtain a copy of her (processed) personal data and you have 30 days to respond.
- Should this right be interpreted broadly? Likely not, the right is limited to personal data of the employee concerned and should not impact negatively the rights and freedoms of other parties e.g. business secrets of the employer, other employees.
- Request could be refused by the employer if it relates to large files in which the employees' personal data appears (e.g. large amount of e-mails with other parties, evaluation form with internal notes ,etc.).
- Notwithstanding restricted right, the exercise of the latter by an employee or ex-employee can lead to a lot of administrative burden (checking all the relevant documents to assess whether the request is acceptable).

Ascender sdworx

Example 4: International payroll

We are working with various local service providers for ensuring our payroll in various EU offices.

How can we make sure that all these service providers are GDPR compliant and that we do not face increased risk?

Ascender sdworx

Example 4: International payroll

- Review your contracts with all the providers and make sure these include a data processing agreement that is fully GDPR compliant
- Assess GDPR compliance of your EU payroll providers through a questionnaire and make sure you only work with providers that can provide the required assurance
- Evaluate if you could further reduce risk and the compliance burden by consolidating and reducing the number of different EU payroll providers

Ascender sdworx

Payroll Services Alliance: a common GDPR compliant approach

Ascender sdworx

We are united

- Network of trusted payroll services partners with GDPR compliant HR and payroll solutions
- Common data privacy framework and data processing agreement ensuring GDPR compliance between all partners in the Payroll Services Alliance
- Strong privacy foundation taking privacy protection seriously starting from building trust as a basis
- Security & privacy specialists that will help you keep-up with the constantly changing regulatory environment for your HR data

Partnership with leading payroll services providers:
SD Worx, Aditro, Ascender, Ceridian, Elanor, F2A, Seresco

Ascender sdworx

Strong data privacy foundation

- Understanding which data is collected, where it is stored and for which purposes it is processed
- Keeping data collected to the minimum required for the services delivered
- Data privacy is a standard part of our services agreements and is built-in from the start
- An HR workforce trained and educated on importance of privacy protection
- 3rd party/partner management programme that takes into account data privacy controls and that enforces GDPR requirements in subcontractor relations

Key Takeaways

- Embrace all privacy laws – don't run from them
- Privacy is first and foremost a compliance issue
- Build your privacy compliance foundation – based on more restrictive laws
- Understand importance of privacy due diligence
- Know the difference between privacy and security
- Implement a breach notification and remediation plan
- Be a privacy evangelist and help solidify your organization's reputation as a proponent of privacy compliance
- Turn privacy compliance into a competitive advantage – build trust

Thank You!

Sheila M. FitzPatrick | sfitzpat@hrglobal.com | @sheilafitzp
Gert Beeckmans | Gert.beeckmans@Sdworx.com | @GertBeeckmans

Ascender

www.ascenderhcm.com

sdworx

www.sdworx.com

Payroll Services Alliance

Ascender sdworx

Global Data Privacy Laws – Ripple Effect of GDPR

Sheila M. FitzPatrick

WORLDWIDE GDPR CHIEF PRIVACY OFFICER, DATA PRIVACY & SOVEREIGNTY LAWS

Gert Beeckmans

CHIEF RISK AND SECURITY OFFICER, SD WORX

CLICK HERE TO VIEW RECORDING

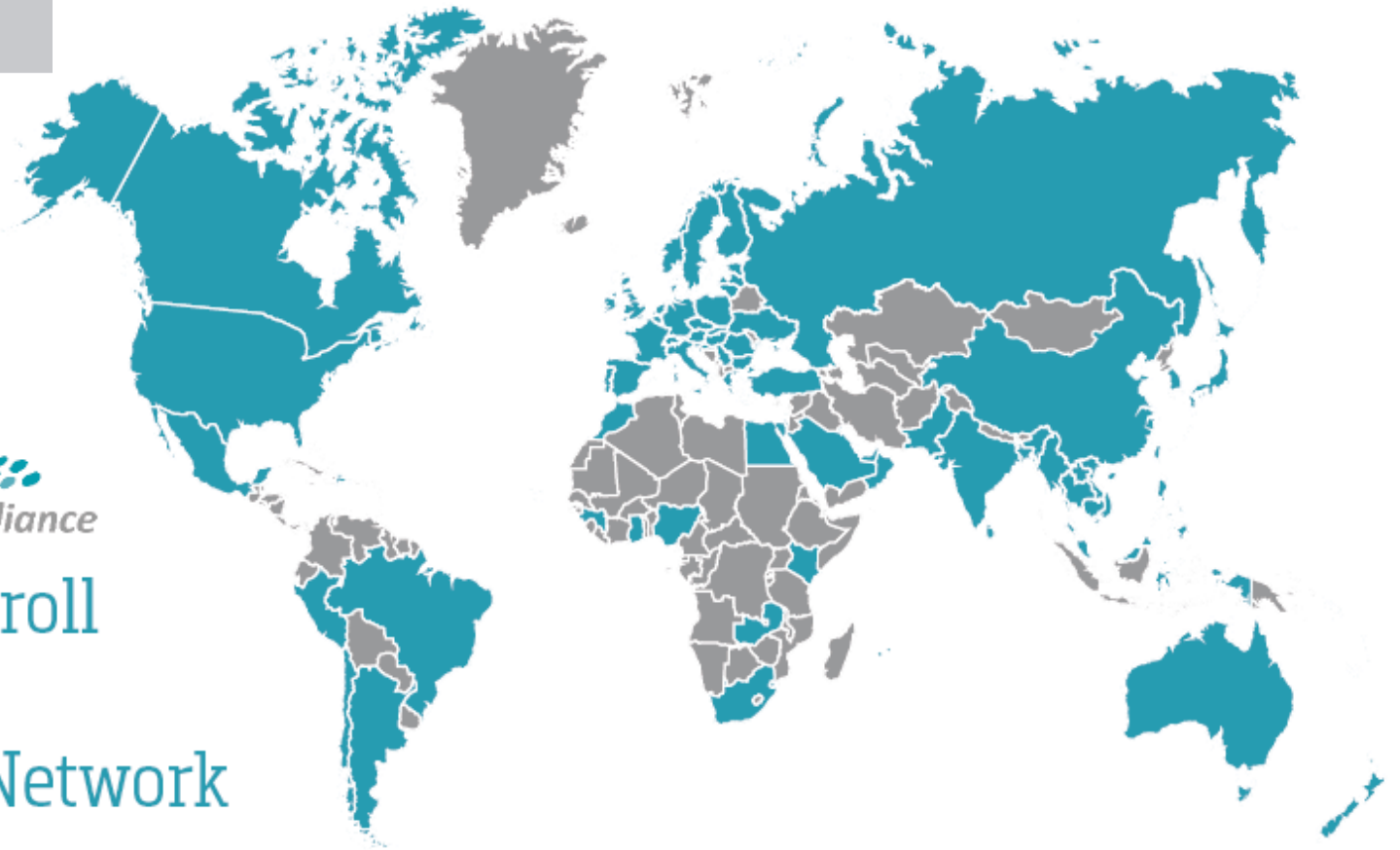
Payroll Services Alliance

www.payrollservicesalliance.com

The Payroll Services Alliance is a network of payroll services companies across Europe, the US, Canada, Asia-Pacific and the Middle-East which can guarantee a consistently high level of payroll service around the world. The Payroll Services Alliance is the second biggest payroll vendor globally, with seven leading payroll service companies working together, namely Aditro, Ascender, Ceridian, Elanor, F2A, SD Worx, Seresco.

Ascender sdworx

Established in 2010



Payroll Services Alliance

Global Payroll Coverage & Partner Network

● Strategic Payroll Services Alliance Partners

Partnership with leading payroll services providers:
SD Worx, Aditro, Ascender, Ceridian, Elanor, F2A, Seresco

+ € 1,600 million
combined revenues

+ 13,000
employees

+ 130,000
customers

+ 32 million
payslips per month