出國報告（出國類別：會議）

出席德國 2017 隱私及個人資料保護高峰會出國報告書

服務機關：國家通訊傳播委員會

姓名職稱：喬建中 專門委員

王維年 科長

派赴國家：德國

出國期間：106 年 11 月 15 日至 106 年 11 月 19 日止

報告日期：106 年 12 月 20 日

出國報告摘要

歐盟即將自 2018 年 5 月 25 日起實施更嚴格的個人資料保護規則（General Data Protection Regulation, GDPR），影響層面包括監理機關，有蒐集用戶之事業體，處理及利用單位，被蒐集個資之當事人，本會為通訊傳播監理機關，對此新規定之施行前後相關準備工作，及是否對產業影響及新的契機，須預做準備，首先須了解世界上各國對 GDPR 的調適及發展，以作為本會監理政策擬定之參考。

GDPR 未來實施前後，有關產業或監理機關是否準備好？大會邀請 eBay、Microsoft、OneTrust…等等公司代表介紹案例後，讓我們深切了解不管公務機關或非公務機關在調整個資管理制度時，應從組織全景著手，並先確認是否已進行「適用法規盤點」、「作業及特定目的盤點」、「個人資料盤點」、「資料流分析」以確認組織是否將整體之法規風險及作業風險皆已納入考量。

另針對個資安全、個資長(Data Protection Officer, DPO)腳色及組織如何轉型，以因應外界的威脅及檢討資料安全保護及流程漏洞檢測，亦即任何資訊系統接存有不安全性，如何減輕網路駭客入侵或勒索軟體之危害程度，可選擇較佳技術，做好防火牆作業及擬定災害發生時應變標準化流程，可於事情發生時將災害減至最輕。早期設置 CISO，負責組織內安全規劃工作，現今改為 DPO 設置，相同定位 DPO 為專業腳色，從事工作定有相當規範，並能不受外力、預算及其他因素干擾，能獨立行使職權，對組織內資料保護工作為關鍵要角。

面對數位經濟環境下，對於通訊傳播產業之相關隱私權及個資保護須配合提升，尤其是電子隱私(e-Privacy)認知及強化，如何在國內或國際相關個資法規及環境底下，建構符合規定及有益健全制度或產業

發展之措施，並配合辦理相關教育訓練或宣導活動，提升組織所有同仁對 GDPR 之認知，進而創造產業動能、增加消費者信任及提升品牌形象。

關鍵詞：GDPR、DPO、e-Privacy

目　錄

壹、目的

本次高峰會議為因應歐盟將於2018年5月25日實施GDPR，關於實施前後相關準備及因應作為。會議主席為馬丁(Martyn Hope)，他的長期合作夥伴基尼克布萊克(Gini Blake)是 GDPR 研究所的創始人。馬丁在IT業有30年的經驗，曾為全球最大的IT供應商工作，在2008年下半年，基尼的線上個人資料防護被攻破，她所有的個人資料都被偷了。當時，基尼領導著一家成功的顧問公司，資料洩露對她個人和職業生涯的影響都是災難性的。這使得馬丁在他廣泛的IT專業人員網路中開始接觸到資訊治理、網路和資訊安全以及資料保護方面的專家。在2014年馬丁和基尼被引入了一個新的歐盟法規起草小組，其重點是確保公司必須遵守更嚴格的資料保護規則，以確保其組織和個人，如同基尼，不再遭受她過去所遇到的棘手問題。

在收集了一個關於資料保護的專家網路後，馬丁和基尼制定了一個計畫，建立一個網路，協助中小型和大型組織應對保護客戶、員工和供應商，並在過程中保護個人的利益。該研究所的創始委員會由許多專家組成，該研究所的諮詢委員會不斷累增實力，現在包括許多全球精神領袖參與及所有的資料保護事項。

在 2016 年初，隨著 GDPR 即將施行，GDPR 研究所在瑞士成立，現已在全球鋪開。該研究所是以非營利為基礎的成員，有數萬名成員，其中許多人是治理、安全和隱私權方面的專家，從諮詢、技術、法律、培訓、智庫和審計等背景，換言之，一切我們的組織可能需要解決 GDPR 的挑戰，它是一個機會，大家共同的目標是：組織如何導入 GDPR。

大會主辦機構為 Luxatia International，它是一個專業活動企劃之機構，員工人數約 50-200 人，總公司在捷克布拉格，平時即擁有專業訓練講師，並可邀請各大學、業界、機關構…等等專業人員，於研討會上擔任講師，每年辦理相關領域之高峰會、年會、研討會或訓練課程。相關辦理課程會後於臉書、推特、Google+或 LinkedIn 上發表，GDPR 學院及主辦單位活動相關連結如下[1]。

另外本次會議鑽石級贊助廠商為 OneTrust，它是一個領先的隱私管理軟體平臺，全球有超過 1500 組織使用，以遵守跨轄區的資料隱私法規，包括歐盟 GDPR。

通過深入的隱私研究， OneTrust 提出綜合集成平臺，包括準備評估、隱私影響評估 (PIA/DPIA)、資料對應自動化、網站掃描和 cookie 遵從性、主題許可權和同意管理，附隨報告和供應商風險管理。讓參與高峰會議學員藉由 OneTrust 經驗分享，可以有系統認知整體隱私及個資保護相關流程及方式，再加上其它單位代表分享，更能了解理論與實務。

貳、會議行程

一、 時間：106 年 11 月 15 日至 19 日

二、 地點：德國柏林

[1] https://www.gdpr.associates/
https://www.facebook.com/luxatiainternational
https://plus.google.com/108463389014473479754
https://www.linkedin.com/company/luxatia-international
https://twitter.com/Luxatia_intl
http://www.luxatiainternational.com/blog/
http://www.luxatiainternational.com/

三、 出席會議人員：說明如表 1 及圖 1、圖 2

出席人員與職銜一覽表

編號	所屬單位	姓名	職銜
1	國家通訊傳播委員會	喬建中	專門委員
2	國家通訊傳播委員會	王維年	科長

圖1 2017 PDPS 綜合座談及會場

圖2 2017 PDPS 高峰會議舉辦的飯店

參、會議內容摘要

一、 議程

表1　11 月 16 日議程

時間	議　　題
16 日 上半 場	**主題**：探討 GDPR 內容和為 2018 年 5 月實施前準備
	1. How to Build and Scale Your Data Mapping Process to Meet GDPR Article 30 Record Keeping Requirements (OneTrust 銷售副總經理 Kevin Kiley) 2. Navigating the EU Regulatory landscape: emerging data and privacy issues and compliance considerations (Microsoft 歐盟政府部門處長 Jeremy Rollison) 3. The GDPR and data-driven innovation: Certificates and codes of conduct as trust anchors (網際網路與社會機構 Maximilian von Grafenstein) 4. Data protection in EU and in Switzerland (Governance.land 獨立董事 Leonardo Scimmi) 5. 7 Months left －How to get things done if you just stumbled over the GDPR and realize there’s a lot to do (Ernst & Young Law GmbH 副合夥人 Jyn Schultze-Melling)
16 日 下半 場	**主題**：GDPR 和您的業務：加快資料保護順序以向前邁進
	1. Implementing The GDPR & Leveraging Privacy as a Competitive Advantage (Ebay 資料保護官員 Anna Zeiter) 2. GDPR in the IoT: how ‘technical measures’ required by the GDPR may be tackled (NXP 半導體公司公共事務組長 Jacques Kruse Brandao) 3. Preparing for Litigation under the GDPR THE Companies’ perspective (WilmerHale 合夥人 Martin Braun) 4. Data Protection Target Operating Model. Is the DPO the only (or best)

時間	議　　題
	option? (Adecco Group 群組隱私保護人員 Anny Pinto) 5. 小組討論: How GDPR can bring value to your business

表2　11 月 17 日議程

時間	議　　題
17 日上半場	**主題**：選擇最佳技術以對抗網路威脅
	1. How to protect your data; a pragmatic approach' – (lessons learned from a former CISO) (Palo Alto Networks, Fred Streefland) 2. WannaCry, Petya/NotPetya, etc.: Putting the Spotlight on Data Protection and Privacy (Credit Suisse 律師事務所 Paul Lanois 律師)
17 日下半場	**主題**：DPO 的角色轉變與組織變革
	1. Data Protection Officer who needs them, why, benefits, challenges and the future. (IBM Watson Health, Stewart Thompson) 2. How GDPR issues handled in GSM/Telco World (Vodafone Turkey 高級經理 Mustafa Komut) 3. GDPR: Time to Evolve (Bruce & Butler Limited, Matt Bruce) 4. Consent in Direct Marketing. (DAMM Solutions, Andy Chesterman) 5. How privacy by design can be the key of the success at the time of the digitalization (DLA Piper 合夥人/律師 Giulio Coraggio) 6. 總結討論: The Role and Responsibilities of a Data Protection Officer and his/her team

二、 高峰會重點摘要分享

GDPR 產生之強制義務及層級化的因應對策如下：

(一) Checklists: GDPR §83.4/ 83.5(administrative fine list),將 GDPR 法遵義務做成清單,不過範圍極為廣泛,涵蓋半數以上條文。

(二) 三種因應 GDPR 義務之 compliance 對策

1. 企業內部自行調整: Microsoft/ eBay/ IBM/ Adecco
2. 業務外包: 多樣化新興產業
   (1) Technical measures: Cyber security/ Data tools
   (2) Organizational measures: DPO (§37-39)
   (3) Certificates and Codes of Conducts: 適格主體 §40.2, 43
   (4) Total solution: OneTrust/ Microsoft
   (5) Consultant
3. Lawsuits
4. 基於企業規模是 GDPR 裁罰所應認定的標準，什麼都不作等著被告，未必是不理性選擇。

高峰會重點摘要如下：

(一)探討 GDPR 內容和為 2018 年 5 月實施前準備

1. 從公司業務流程設計的角度列舉重要 GDPR 義務在 Data-driven industry，紀錄 Data Mapping 是相關義務被履行的前提(Kevin Kiley, OneTrust 銷售副總)
   (1) 符合 GDPR 要求之相關議題及條文如下:
   - Legal Basis for Processing (§6)
   - Policy, Notice, Transparency(§13)
   - Data Protection by Design and Default(§25)

- Data Protection Impact Assessments(§35)
- Joint Liability with Vendors and Sub-Processors(§28)
- Data Protection Officer Tasks(§39)
- Consent Obligations (§7)
- Cookie, Online Tracking, and Marketing Reform(ePrivacy)
- 72 Hour Data Breach Reporting(§33,34)
- Records of Processing Activities(§30)
- Data Portability and Erasure (Right to be Forgotten) (§17,20)
- Subject Access Rights(第 3 章)
- International Data Transfers(第 5 章)
- Codes of Conduct and Certifications(§40,42)
- Security Balancing Risk, State of Art, Cost(§32)

(2) Records of Processing Activities

- Controller 需自證行政義務的履行/ 民事推定過失責任。
- 既有的資料庫不能滿足新的法律要件要求，eg. Categories of personal data。
- 履行紀錄義務的要件：包括 Team staff : privacy office, legal, IT, and records management, Standards and Tools。
- Data-driven 組織結構改造 (by Sensitivity/ Risk)

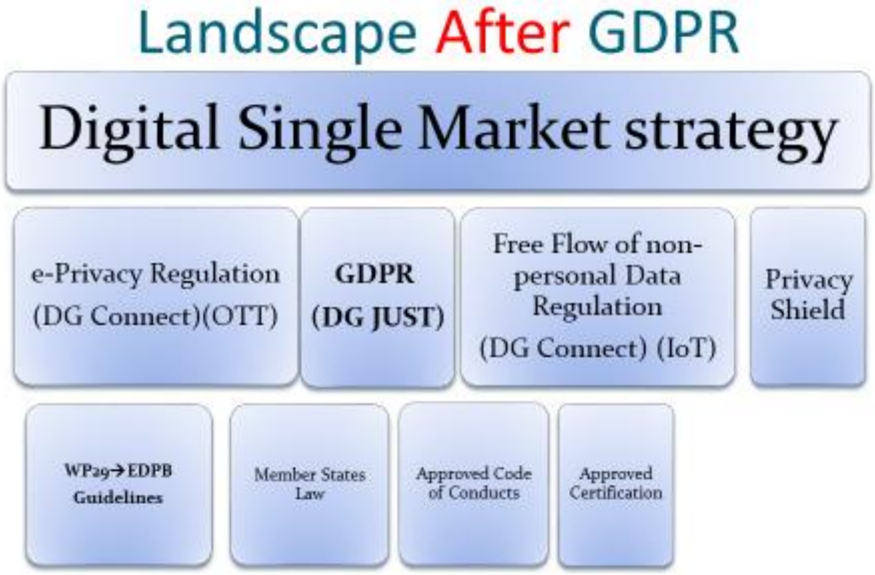
- 為什麼 RoPA 很重要的兩條法律義務路線 (行政/ 民事)，資料庫翻新需靠 staff +新工具(不是人力就可以完成的)。

2. GDPR 與整體 EU 網路政策部局(Jeremy Rollison, EU Government Affairs Microsoft Director)

(1) 先前是在 Brussels 負責遊說，GDPR 通過改負責 compliance / compliance tools marketing

(2) Landscape after GDPR：包括 Digital Single Market strategy，e-privacy 及 free flow of data 等 3 層次。

(3) Microsoft 在 GDPR 準備花了半年，投入 300 人力，為確保 Microsoft 符合之後，可使客戶利用此經驗及雲端工具服務以符合 GDPR 要求。



Landscape After GDPR

Digital Single Market strategy

e-Privacy Regulation (DG Connect)(OTT)

GDPR (DG JUST)

Free Flow of non-personal Data Regulation (DG Connect) (IoT)

Privacy Shield

WP29→EDPB Guidelines

Member States Law

Approved Code of Conducts

Approved Certification

3. 從上圖 Landscape After GDPR 來看，可得以下結論：

(1) e-privacy 背景：電信商覺得在與 OTT 的競賽中，GDPR 偏向 OTT pushing for level playing field (預計明年二月通過，五月生效)。

(2) 把 OTT 0-2 均納管， OTT (ECS)。

(3) Metadata 是處理重點。

(4) 以台灣的例子: 大規模真正利用個資的是 Line、 FB messenger , 但是我們只對幾乎沒有 metadata 的五大電信業者進行資安或個資進行行政訪查。

(5) Free flow of data regulation sept 2017：有些會員對於 EU 境內的資料移轉也有疑慮，對於 localization 採最嚴格的態度，這對 DSM 雲端產業有相當不利之影響。

(6) Privacy shield 執行的前景還是相當不明。

4. GDPR 之 Certificates and Codes of Conducts (Maximilian von Grafenstein)

(1) GDPR 與 Data-driven innovation 的本質矛盾性: knowledge uncertainties

- 預設的特定 Purpose 是所有資料處理的前提要件。
- Innovation 的特徵是發現目的以外的 knowledge。

(2) 為處理 knowledge uncertainties 造成的第二層矛盾: legal uncertainty

- 大量採用不確定法律概念 (eg. §25.1)
- 產業不知道什麼行為可做，消費者不知道什麼產品可買。

(3) 緩和兩種矛盾創造信任的緩衝機制

- Code of Conduct (§40,41)
- Certification (§42,43)

(4) 被 SA 或 EDPB 認可的 Code of Conduct 與 Certification 在某些條文具有義務履行的表面證據效力(eg. §28.5, 32.4)；執行主體具有監督權(§41-43)，違反有行政罰(§83.4 b,c)。

(5) §25.1 Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

5. GDPR 的底線準備（Ernst & Young）

(1) GDPR 的 Compliance 不是 0/1 的問題：

- GDPR 的義務的多樣性。
- 官員不會知道你們企業的內部狀態，但一定會要你交出各種文件，所以形式要件一定要符合。

(2) 企業應自我評估找出優先推動目標：

- （被告）風險評估。
- Compliance 成本評估。
- 80/20 法則 (Pareto principle)。

(3) 底線準備：

- Documentation (RoPA, DPIA, various Schedules…)
- Data subject request

(4) 連底線準備都做不到的時候： Try to justify your legitimate interests (eg. § 6.1 f)。

(5) 法遵不是 0 與 1 的問題。

(6) 企業應該有〔合理的〕Budget 投入，而不是盡全力做好。

(二)GDPR 和您的業務：加快資料保護順序以向前邁進

1. GDPR Compliance 執行經驗—eBay

(1)企業資料儲存概況：它的國際總部在瑞士，Main establishment in EU 在盧森堡，除北美跟歐洲以外的 data 儲存在瑞士。

(2)本報告提供 Compliance Road Map

(3)2014 Data Breach 事件

(4)在與 Amazon / Alibaba 的競爭中節節敗退，所以 GDPR 既是危機也是轉機(跟 Microsoft 的情境類似)。

(5)GDPR Compliance Road Map

- Part I – Preparation (January 2016 – March 2016)
- Part II – Gap Analysis (April 2016 – August 2016)
- Part III – Budget/Resource Planning (September 2016)
- Part IV – Implementation (October 2016 – December 2018)
- Part V – Monitoring (October 2017 – December 2018)

(6)執行期跨越 GDPR 生效實施日: 表示在生效日前，eBay 並未 100% 完成 compliance。

(7)這不是一個 0/ 1 的問題，而是比例原則下努力程度的問題。

(8)Monitoring 與 Implementation 成為一個循環過程: 邊走邊

看，主要看 EU 與競爭者的互動。

(9)List of Action Items(selected)

- Data mapping
- Process for new subject access rights
- Privacy Impact Assessments (PIAs)
- Privacy by design/by default
- Review of consent based processing
- Review of the DPO position
- Privacy champion program
- Data deletion/data retention
- Data breach response plan
- Privacy trainings

2. GDPR 要求的”Technical Measures”(Jacques Kruse Brandao, NXP 半導體公司公共事務事務組長)

(1)NXP 為晶片製造商，許多 IoT 晶片儲存 Personally identifiable information (PII)，如何保護其安全，為該公司 GDPR 重點工作。

(2)挑戰：

- 要求採取合理的技術措施在 GDPR 出現 14 次，核心條文§ 32 : the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security.
- Security 在 GDPR 出現超過 50 次，但也沒有定義。

- “State of the Art”成為判定是否採用 appropriate technical measures 的標準。

(3)Solutions:

- GDPR 具高度法律不確定性 (參考§ 32 .1 主文)。
- 由於發明週期越來越短，何謂安全越來越難確定，也無法標準化。
- 不斷提高自我的標準，創造最高標準的“State of the Art”是 NXP 的目標。

(4)Q&A

- Q: IoT device 會因為個資安全問題被禁止嗎？
- A :重點應該是誰要為甚麼事負責？這一行的產業鍊非常長，責任關係很難釐清。

(5)NXP 介紹內部超過 70+的安全需求 checklist。

(6)§ 32 .1 主文：Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons，最高標準的“State of the Art”隱含市場領導者可以基於技術優勢更加容易排除次級競爭者。

3. GDPR 相關的訴訟（Martin Braun, Wilmer Hale 合夥人）

(1)GDPR 新增的三種訴訟類型：

- 行政訴訟：任何人得對 SA 提起行政救濟(§ 78)
- 給付之訴：資料主體對於控制者與處理者主張履行 GDPR 上之義務 (§ 79)

- 損害賠償之訴：任何人得對控制者與處理者主張侵權行為損害賠償 (§82)

(2)集體訴訟 (§80)

(3)跨境訴訟之管轄 (§81)：一體化為 GDPR 之主要目標，多重手段（consistency mechanism (§ 63)/ Main Establishment/ Lead SA/ 優先管轄）。

(4)如果準備不足，就等著被告。

(5)不過預估會被告的，應該是準備最充足的(Google , FB)。

(6)§ 63 並且為其他十幾個條文之要件。

(三)選擇最佳技術以對抗網路威脅

1. Cyber Security Project (Fred Streefland, Palo Alto Networks)

(1)Paloalto 核心產品為「下一代防火牆」(Next-Generation Firewall) 平臺(自稱)。

(2)Cloud-based security 是 Data-driven industry 的必要條件。

(3)Step-by-step security plan (公司產品介紹)。

(4)客戶數量/反應速度 決定雲端安全防護的 Capacity (隱含大者恆大的推定)。

(5)Problem: Privacy 與 security 之間的優先保護選擇本身就造成 security 的問題？

(6)Step-by-step security plan

- Get to know your IT environment
- Provide Security awareness training for all personnel
- Develop Information Security policies & Incident Response Plan

- Implement perimeter security & internal segmentation
- Install Next-Gen firewalls & use the Threat Intelligence Cloud
- Implement two-factor authentication
- Protect & manage Endpoints
- Implement Cloud security (Aperture)

(四)DPO 的角色轉變與組織變革

1. DPO 的需求、理由、利益、挑戰及未來 (Stewart Thompson, IBM Watson Health)

(1)GDPR 新增企業強制 DPO 要件 (§ 37.1 c)：

- Large scale processing
- Regular and Systemic Monitoring

(2)DPO 的重要特徵：

- 需有內國法及 GDPR 之專業及實務經驗。
- 不能有利益衝突問題。
- 不能是定期或短期約僱 (WP 29)。
- 不應該向最高層以外的主管負責報告。

(3)估計市場上 DPO 的需求為 75,000+, 但無此種供給。解決方案: 各類”創意”供給可能產生。

- DPO 在 GDPR 37-39 有相當清楚的規範，看法條可瞭解。
- DPO 在 WP29 時代(非強制義務)已建立許多 guidelines, 具體認定標準應從 WP29 著手。
- 各國法未來是 DPO 的重點。

肆、心得及建議

基於 GDPR 的法規複雜性與快速技術演進，各方對未來實施狀況有不同預測。從 GDPR 的層級化保護結構與數位單一市場的目標觀察：

一、 GDPR 實施之可能方向：

(一)執行成本極高，目標必須限定。

(二)大型跨境雲端計算公司是假想目標。

(三)對周邊國家有較大影響(UK，瑞士，土耳其)。

二、 GDPR 對我國國內法之啟示：

(一)從分工來看，DG JUST 與 DG Connect 有不同價值取向，上層共同概念是 DSM，後續電信營運商、OTT、IoT 業者都會捲入。

(二)Level playing fields：有必要從義務內容到構成要件均區分。

(三)正確的 Awareness 與排定 Priority 是一切的基礎。

三、 國內業者之因應：

(一) 消極性: 基於 GDPR 有部分跨境效力(§2.1 a), 與 EU 業務密切相關之產業均應了解其內容，再依產業資料密集度確認所需因應方案。

(二) 積極性: GDPR 提供了進入資料密集產業所需的 Road Map, 主動 Compliance 提供企業從組織到 work flow 全面改造的機會

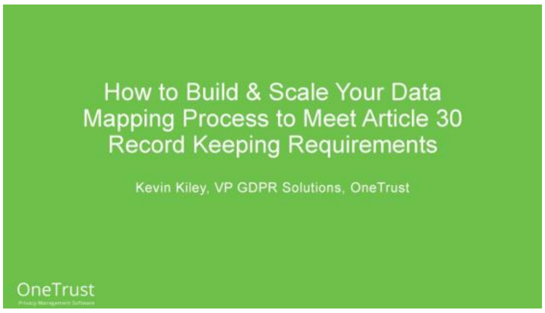
四、 不同 Paradigms 間競爭對我國的影響

(一) 跨境資訊流限制越多，網路分裂(Splinternet/ Balkanization)可能性越來越高。

(二) GDPR 具有高度預設理性，但 EU 在數位經濟不是領先者。

(三) Privacy Shield/ CBPR 在我國可能更有優先急迫性。

附錄－會議簡報資料



How to Build & Scale Your Data Mapping Process to Meet Article 30 Record Keeping Requirements

Kevin Kiley, VP GDPR Solutions, OneTrust

OneTrust
Privacy Management Software

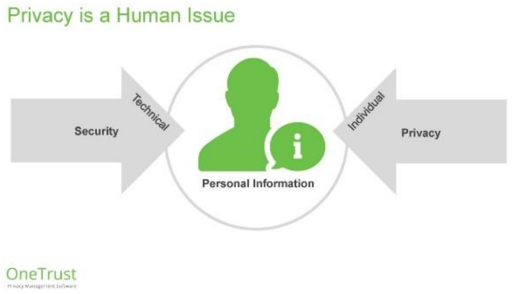
Agenda

1 | Impact of GDPR

2 | Who is Doing the Work

3 | 10 Steps

OneTrust
Privacy Management Software



Privacy is a Human Issue

Security

Technical

Personal Information

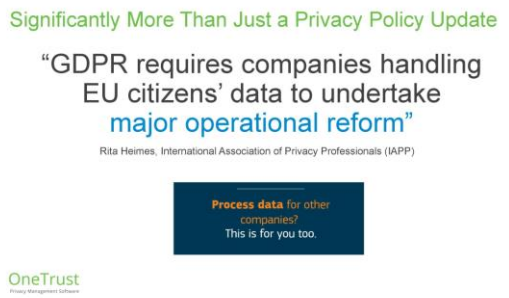
Individual

Privacy

OneTrust
Privacy Management Software

Impact of the GDPR

OneTrust
Privacy Management Software



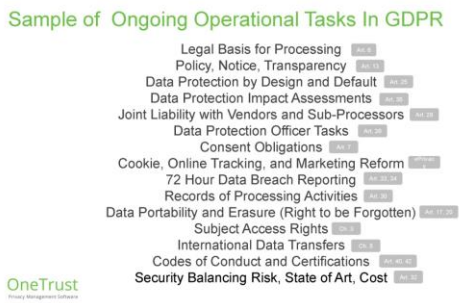
Significantly More Than Just a Privacy Policy Update

"GDPR requires companies handling EU citizens' data to undertake major operational reform"

Rita Heimes, International Association of Privacy Professionals (IAPP)

Process data for other companies?
This is for you too.

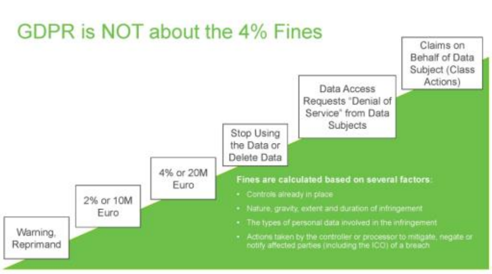
OneTrust
Privacy Management Software



Sample of Ongoing Operational Tasks In GDPR

Legal Basis for Processing Art. 6
Policy, Notice, Transparency Art. 13
Data Protection by Design and Default Art. 25
Data Protection Impact Assessments Art. 35
Joint Liability with Vendors and Sub-Processors Art. 28
Data Protection Officer Tasks Art. 38
Consent Obligations Art. 7
Cookie, Online Tracking, and Marketing Reform ePrivacy
72 Hour Data Breach Reporting Art. 33, 34
Records of Processing Activities Art. 30
Data Portability and Erasure (Right to be Forgotten) Art. 17, 20
Subject Access Rights Ch. 3
International Data Transfers Ch. 5
Codes of Conduct and Certifications Art. 40, 42
Security Balancing Risk, State of Art, Cost Art. 32

OneTrust
Privacy Management Software



GDPR is NOT about the 4% Fines

Warning, Reprimand

2% or 10M Euro

4% or 20M Euro

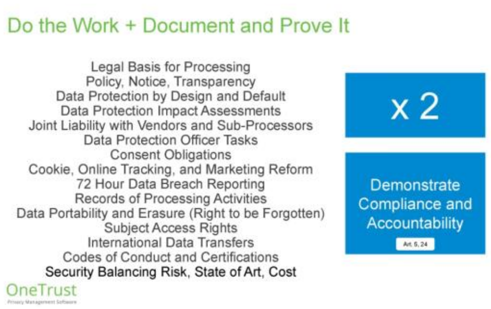
Stop Using the Data or Delete Data

Data Access Requests "Denial of Service" from Data Subjects

Claims on Behalf of Data Subject (Class Actions)

Fines are calculated based on several factors:

- Controls already in place
- Nature, gravity, extent and duration of infringement
- The types of personal data involved in the infringement
- Actions taken by the controller or processor to mitigate, negate or notify affected parties (including the ICO) of a breach



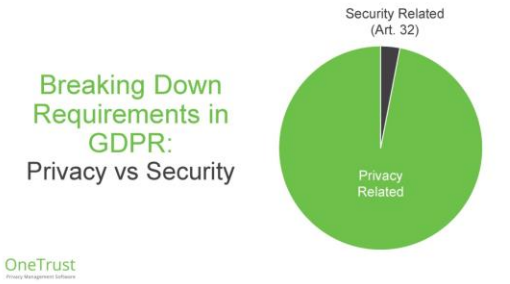
Do the Work + Document and Prove It

Legal Basis for Processing
Policy, Notice, Transparency
Data Protection by Design and Default
Data Protection Impact Assessments
Joint Liability with Vendors and Sub-Processors
Data Protection Officer Tasks
Consent Obligations
Cookie, Online Tracking, and Marketing Reform
72 Hour Data Breach Reporting
Records of Processing Activities
Data Portability and Erasure (Right to be Forgotten)
Subject Access Rights
International Data Transfers
Codes of Conduct and Certifications
Security Balancing Risk, State of Art, Cost

x 2

Demonstrate Compliance and Accountability
Art. 5, 24

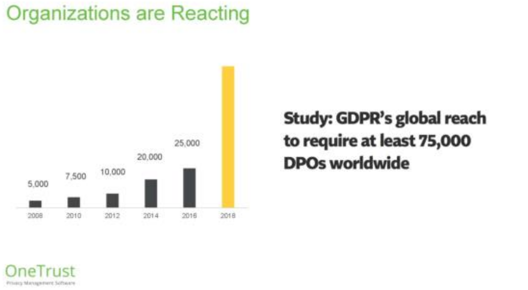
OneTrust
Privacy Management Software



Breaking Down Requirements in GDPR:

Privacy vs Security

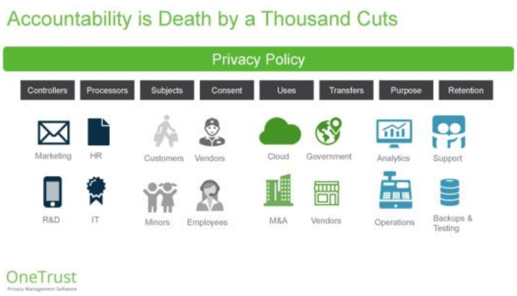
OneTrust
Privacy Management Software



Organizations are Reacting

Study: GDPR's global reach to require at least 75,000 DPOs worldwide

OneTrust
Privacy Management Software

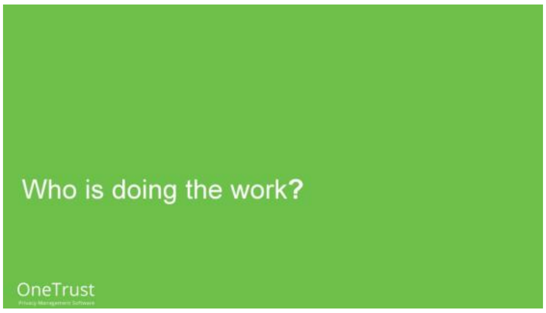


Accountability is Death by a Thousand Cuts

Privacy Policy

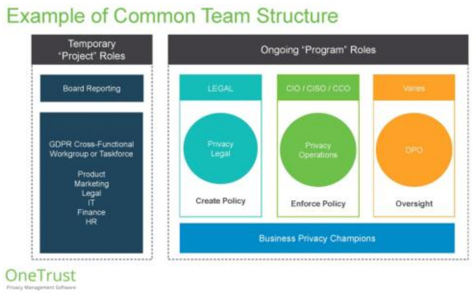
Controllers	Processors	Subjects	Consent	Uses	Transfers	Purpose	Retention

OneTrust
Privacy Management Software



Who is doing the work?

OneTrust
Privacy Management Software

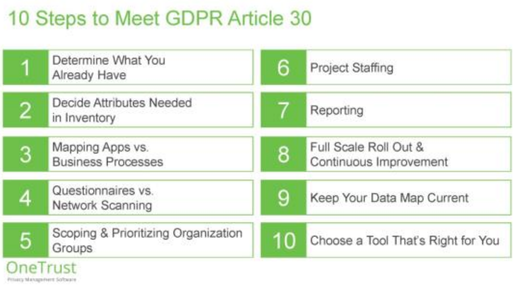


Example of Common Team Structure

OneTrust
Privacy Management Software

10 Steps to Meet GDPR Article 30

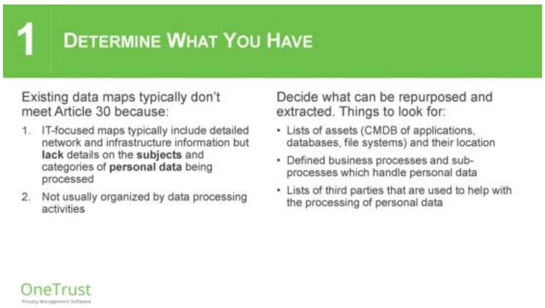
OneTrust
Privacy Management Software



10 Steps to Meet GDPR Article 30

1	Determine What You Already Have	6	Project Staffing
2	Decide Attributes Needed in Inventory	7	Reporting
3	Mapping Apps vs. Business Processes	8	Full Scale Roll Out & Continuous Improvement
4	Questionnaires vs. Network Scanning	9	Keep Your Data Map Current
5	Scoping & Prioritizing Organization Groups	10	Choose a Tool That's Right for You

OneTrust
Privacy Management Software



1 Determine What You Have

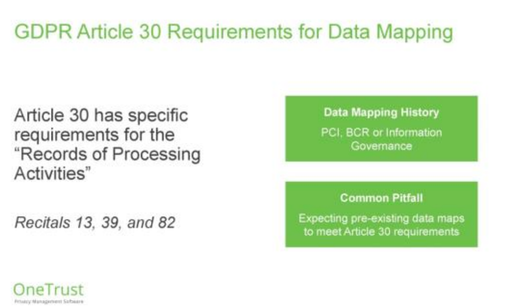
Existing data maps typically don't meet Article 30 because:

1. IT-focused maps typically include detailed network and infrastructure information but **lack** details on the **subjects** and categories of **personal data** being processed
2. Not usually organized by data processing activities

Decide what can be repurposed and extracted. Things to look for:

- Lists of assets (CMDB of applications, databases, file systems) and their location
- Defined business processes and sub-processes which handle personal data
- Lists of third parties that are used to help with the processing of personal data

OneTrust
Privacy Management Software



GDPR Article 30 Requirements for Data Mapping

Article 30 has specific requirements for the "Records of Processing Activities"

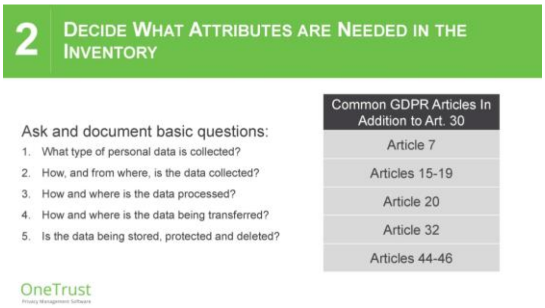
Recitals 13, 39, and 82

Data Mapping History

PCI, BCR or Information Governance

Common Pitfall

Expecting pre-existing data maps to meet Article 30 requirements

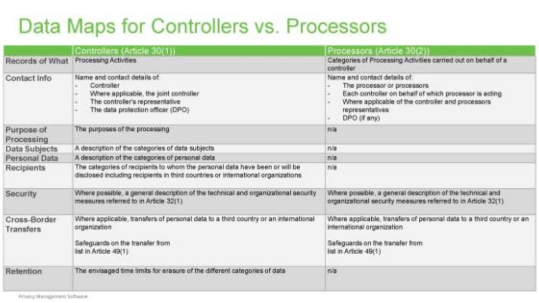


2 Decide What Attributes are Needed in the Inventory

Ask and document basic questions:

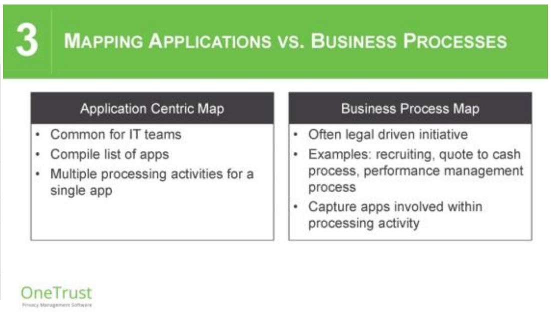
1. What type of personal data is collected?
2. How, and from where, is the data collected?
3. How and where is the data processed?
4. How and where is the data being transferred?
5. Is the data being stored, protected and deleted?

Common GDPR Articles In Addition to Art. 30
Article 7
Articles 15-19
Article 20
Article 32
Articles 44-46



Data Maps for Controllers vs. Processors

	Controllers (Article 30(1))	Processors (Article 30(2))
Records of What	Processing Activities	Categories of Processing Activities carried out on behalf of a controller
Contact Info	Name and contact details of: - Controller - Where applicable, the joint controller - The controller's representative - The data protection officer (DPO)	Name and contact details of: - The processor or processors - Each controller on behalf of which processor is acting - Where applicable of the controller and processors representatives - DPO (if any)
Purpose of Processing	The purposes of the processing	n/a
Data Subjects	A description of the categories of data subjects	n/a
Personal Data	A description of the categories of personal data	n/a
Recipients	The categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations	n/a
Security	Where possible, a general description of the technical and organizational security measures referred to in Article 32(1)	Where possible, a general description of the technical and organizational security measures referred to in Article 32(1)
Cross-Border Transfers	Where applicable, transfers of personal data to a third country or an international organization Safeguards on the transfer from list in Article 49(1)	Where applicable, transfers of personal data to a third country or an international organization Safeguards on the transfer from list in Article 49(1)
Retention	The envisaged time limits for erasure of the different categories of data	n/a



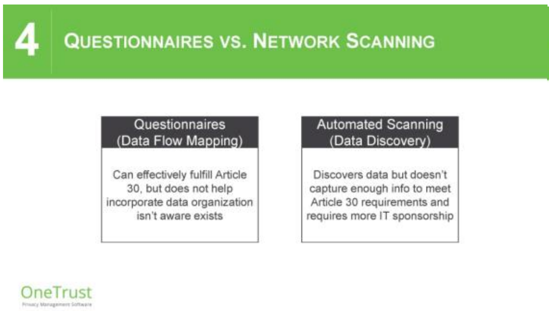
3 Mapping Applications vs. Business Processes

Application Centric Map

- Common for IT teams
- Compile list of apps
- Multiple processing activities for a single app

Business Process Map

- Often legal driven initiative
- Examples: recruiting, quote to cash process, performance management process
- Capture apps involved within processing activity



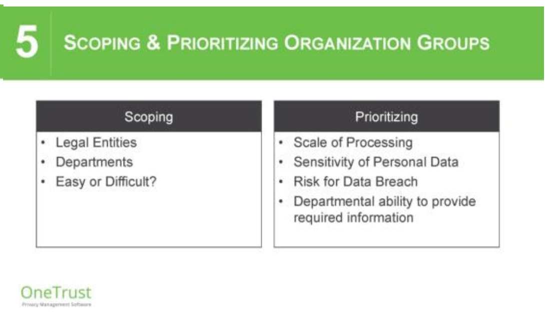
4 Questionnaires vs. Network Scanning

Questionnaires (Data Flow Mapping)

Can effectively fulfill Article 30, but does not help incorporate data organization isn't aware exists

Automated Scanning (Data Discovery)

Discovers data but doesn't capture enough info to meet Article 30 requirements and requires more IT sponsorship



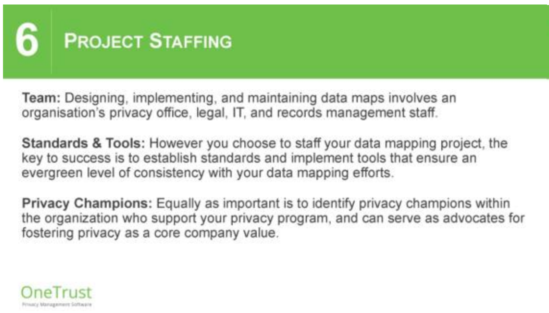
5 Scoping & Prioritizing Organization Groups

Scoping

- Legal Entities
- Departments
- Easy or Difficult?

Prioritizing

- Scale of Processing
- Sensitivity of Personal Data
- Risk for Data Breach
- Departmental ability to provide required information

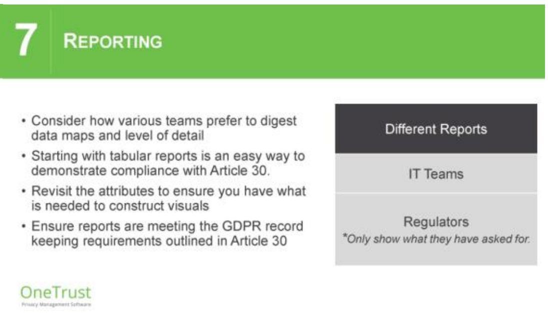


6 Project Staffing

Team: Designing, implementing, and maintaining data maps involves an organisation's privacy office, legal, IT, and records management staff.

Standards & Tools: However you choose to staff your data mapping project, the key to success is to establish standards and implement tools that ensure an evergreen level of consistency with your data mapping efforts.

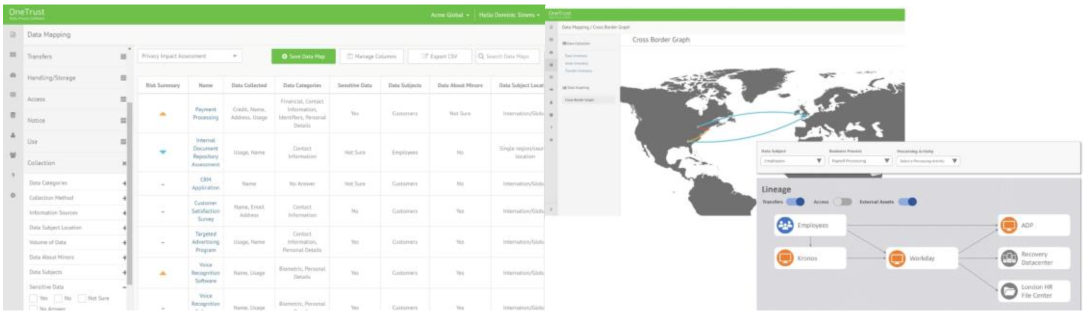
Privacy Champions: Equally as important is to identify privacy champions within the organization who support your privacy program, and can serve as advocates for fostering privacy as a core company value.



7 Reporting

- Consider how various teams prefer to digest data maps and level of detail
- Starting with tabular reports is an easy way to demonstrate compliance with Article 30.
- Revisit the attributes to ensure you have what is needed to construct visuals
- Ensure reports are meeting the GDPR record keeping requirements outlined in Article 30

Different Reports
IT Teams
Regulators **Only show what they have asked for.*



Risk Summary	Name	Data Collected	Data Categories	Sensitive Data	Data Subjects	Data About Minors	Data Subject Locat
▲	Payment Processing	Credit, Name, Address, Usage	Financial, Contact Information, Identifiers, Personal Details	Yes	Customers	Not Sure	International/Glob
▼	Internal Document Repository Assessment	Usage, Name	Contact Information	Not Sure	Employees	No	Single region/cour location
–	CRM Application	Name	No Answer	Not Sure	Customers	No	International/Glob
–	Customer Satisfaction Survey	Name, Email Address	Contact Information	No	Customers	Yes	International/Glob
–	Targeted Advertising Program	Usage, Name	Contact Information, Personal Details	Yes	Customers	Yes	International/Glob
▲	Voice Recognition Software	Name, Usage	Biometric, Personal Details	Yes	Customers	Yes	International/Glob
–	Voice Recognition	Name, Usage	Biometric, Personal	Yes	Customers	Yes	International/Glob

8 Full Scale Roll Out and Continuous Improvement

To ensure that the map you are building is accurate, a **review and approval process** should be put in place for all the data that is feeding into your map.

Tips:

- **Review** incoming questionnaires, API feeds, or scanning results
- Enable **history tracking** for who provided, modified and approved information

OneTrust

9 Keep Your Data Map Current

Ways a Tool Can Help:

- Automated "What's Changed" Audits (Most Common)
- Ongoing PIA and Risk Assessments on New Projects
- Ongoing Vendor Assessments
- Automated Tool to Dynamically Update Visuals Based on Inventory
- Automated Scanning Tools in Parallel

OneTrust

10 Choose a Tool That's Right for You

Things to Consider:

- Level of integration with your various privacy workflows
- Stand alone data mapping vs. comprehensive privacy management platform
- Ease of implementation and user experience
- Scalability across legal entities, departments, regions

OneTrust

Free Tools Available

iapp | OneTrust

DPIA, Data Mapping, and Cookie Compliance Platform

OneTrust.com/IAPP

OneTrust

SmartPrivacy

Local Workshops by OneTrust

Free half-day GDPR workshops for privacy professionals focused on tools and best practices to operationalise compliance

4.5 IAPP CPE Credit Hours

2017 GLOBAL TOUR

Washington DC	Sydney	Brussels
Frankfurt	Milan	Chicago
Seattle	Madrid	Geneva
Dublin	Atlanta	Zurich
San Francisco	Paris	Copenhagen
Denver	Dallas	Stockholm
London	San Diego	Boston
Munich	Philadelphia	Berlin
Hong Kong	New York	Toronto
Vienna	Amsterdam	Minneapolis

RSVP Today | SmartPrivacy.com

Visit Our Booth Downstairs

Product Demos
Full Text GDPR Books
Free Tools & Templates
SmartPrivacy Workshops

OneTrust

Microsoft

Navigating the EU Regulatory landscape: Emerging data and privacy issues and compliance considerations

16 November 2017
Privacy & Data Protection Summit

Jeremy Rollison
Director, EU Government Affairs, Microsoft

"Businesses and users are going to embrace technology only if they can trust it."

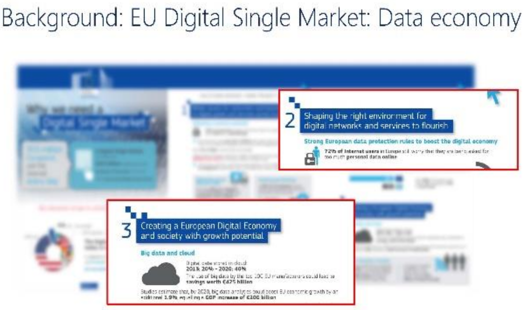
Satya Nadella
Chief Executive Officer
Microsoft Corporation

- We take a principled approach with strong commitments to privacy, security, compliance and transparency.
- Moving to the cloud makes it easier for you to become compliant with privacy regulations by managing and protecting personal data in a centralized location.
- Microsoft is the industry leader in privacy and security with extensive expertise complying with complex regulations.

Political priorities & regulatory, technical realities

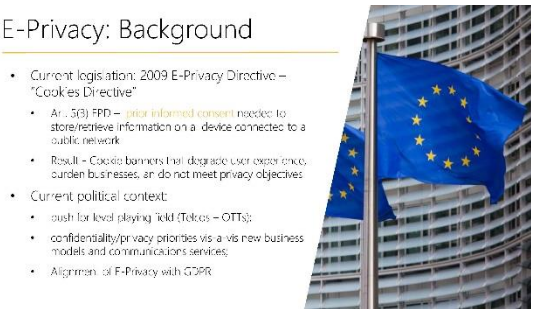
Opportunities - and need for - technical and common understanding

Privacy
Cybersecurity
Cloud
Big Data
Internet of Things



Background: EU Digital Single Market: Data economy

Why we need a Digital Single Market
2 Shaping the right environment for digital networks and services to flourish
Strong European data protection rules to boost the digital economy
72% of internet users in Europe still worry that they are being asked for too much personal data online
3 Creating a European Digital Economy and society with growth potential
Big data and cloud
Digital data stored in cloud
2013: 20% - 2020: 40%
The use of big data by the top 100 EU manufacturers could lead to savings worth €425 billion
Studies estimate that, by 2020, big data analytics could boost EU economic growth by an additional 1.9%, equalling a GDP increase of €206 billion

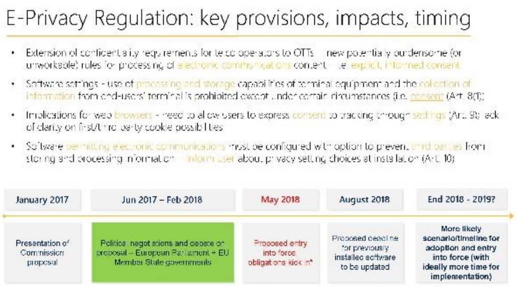


E-Privacy: Background

- Current legislation: 2009 E-Privacy Directive – "Cookies Directive"
  - Art. 5(3) EPD – prior informed consent needed to store/retrieve information on a device connected to a public network
  - Result – Cookie banners that degrade user experience, burden businesses, an do not meet privacy objectives
- Current political context:
  - push for level playing field (Telcos – OTTs);
  - confidentiality/privacy priorities vis-a-vis new business models and communications services;
  - Alignment of E-Privacy with GDPR

EU Policy landscape – 2017

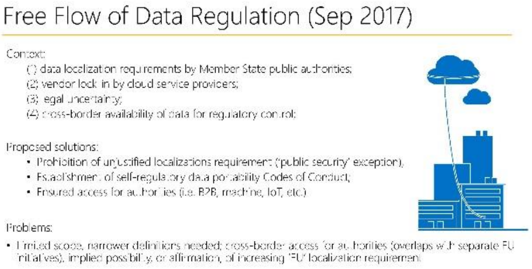
- ~~General Data Protection Regulation (GDPR)~~
  - Compliance readiness, MS implementation DPA guidance
- Proposed E-privacy Regulation
- Proposed Free Flow of Data Regulation
- International data transfers



E-Privacy Regulation: key provisions, impacts, timing

- Extension of confidentiality requirements for telco operators to OTTs – new potentially burdensome (or unworkable) rules for processing of electronic communications content – i.e. explicit, informed consent
- Software settings - use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal is prohibited except under certain circumstances (i.e. consent (Art. 8(1);
- Implications for web browsers - need to allow users to express consent to tracking through settings (Art. 9); lack of clarity on first/third party cookie possibilities
- Software permitting electronic communications must be configured with option to prevent third parties from storing and processing information – inform user about privacy setting choices at installation (Art. 10)

January 2017	Jun 2017 – Feb 2018	May 2018	August 2018	End 2018 - 2019?
Presentation of Commission proposal	Political negotiations and debate on proposal – European Parliament + EU Member State governments	Proposed entry into force obligations kick in*	Proposed deadline for previously installed software to be updated	More likely scenario/timeline for adoption and entry into force (with ideally more time for implementation)

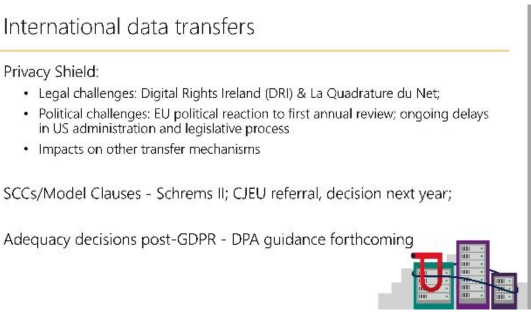


Free Flow of Data Regulation (Sep 2017)

Context:
(1) data localization requirements by Member State public authorities;
(2) vendor lock in by cloud service providers;
(3) legal uncertainty;
(4) cross-border availability of data for regulatory control;

Proposed solutions:
- Prohibition of unjustified localizations requirement ('public security' exception),
- Establishment of self-regulatory data portability Codes of Conduct;
- Ensured access for authorities (i.e. B2B, machine, IoT, etc.)

Problems:
- Limited scope, narrower definitions needed; cross-border access for authorities (overlaps with separate EU initiatives), implied possibility, or affirmation, of increasing 'EU' localization requirement



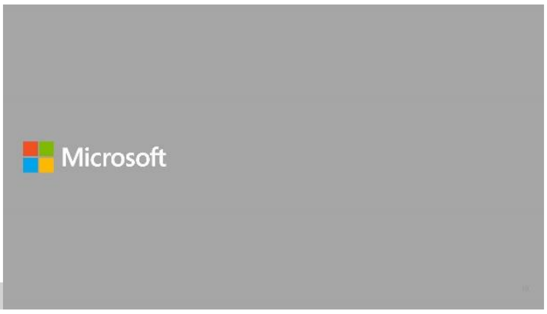
International data transfers

Privacy Shield:

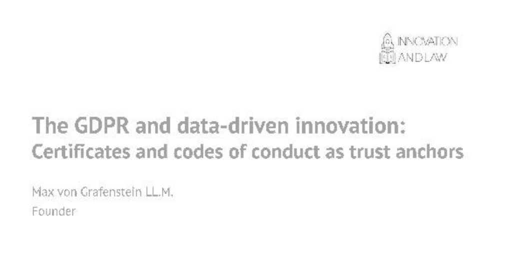
- Legal challenges: Digital Rights Ireland (DRI) & La Quadrature du Net;
- Political challenges: EU political reaction to first annual review; ongoing delays in US administration and legislative process
- Impacts on other transfer mechanisms

SCCs/Model Clauses - Schrems II; CJEU referral, decision next year;

Adequacy decisions post-GDPR - DPA guidance forthcoming



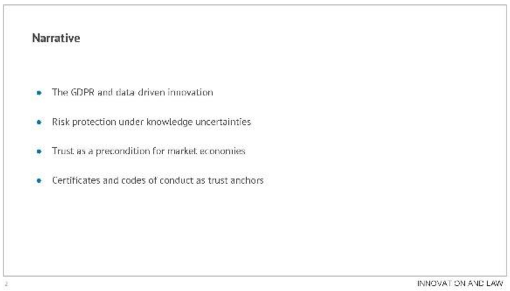
Microsoft



INNOVATION AND LAW

The GDPR and data-driven innovation: Certificates and codes of conduct as trust anchors

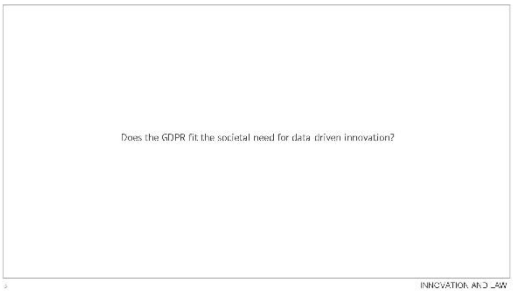
Max von Grafenstein LL.M.
Founder



Narrative

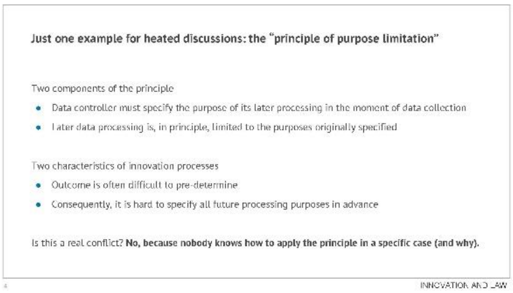
- The GDPR and data driven innovation
- Risk protection under knowledge uncertainties
- Trust as a precondition for market economies
- Certificates and codes of conduct as trust anchors

2 INNOVATION AND LAW



Does the GDPR fit the societal need for data driven innovation?

3 INNOVATION AND LAW



Just one example for heated discussions: the "principle of purpose limitation"

Two components of the principle

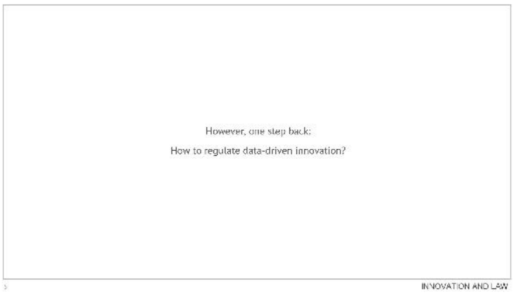
- Data controller must specify the purpose of its later processing in the moment of data collection
- Later data processing is, in principle, limited to the purposes originally specified

Two characteristics of innovation processes

- Outcome is often difficult to pre-determine
- Consequently, it is hard to specify all future processing purposes in advance

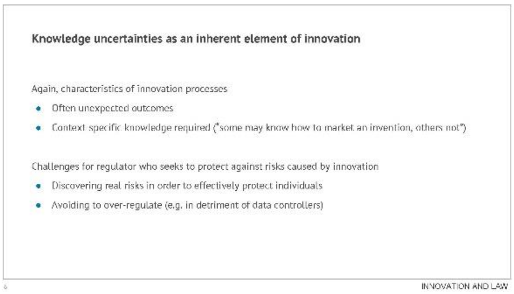
Is this a real conflict? **No, because nobody knows how to apply the principle in a specific case (and why).**

4 INNOVATION AND LAW



However, one step back:
How to regulate data-driven innovation?

5 INNOVATION AND LAW



Knowledge uncertainties as an inherent element of innovation

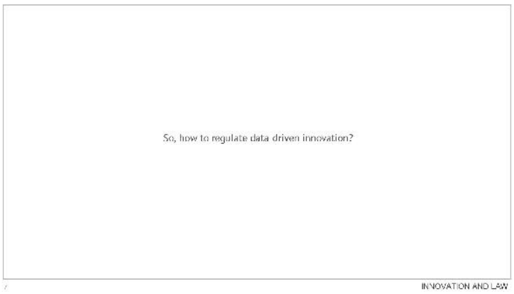
Again, characteristics of innovation processes

- Often unexpected outcomes
- Context specific knowledge required ("some may know how to market an invention, others not")

Challenges for regulator who seeks to protect against risks caused by innovation

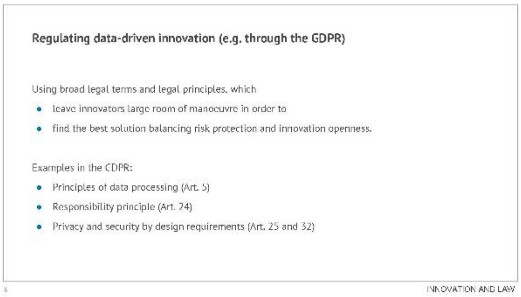
- Discovering real risks in order to effectively protect individuals
- Avoiding to over-regulate (e.g. in detriment of data controllers)

6 INNOVATION AND LAW



So, how to regulate data driven innovation?

7 INNOVATION AND LAW



Regulating data-driven innovation (e.g. through the GDPR)

Using broad legal terms and legal principles, which

- leave innovators large room of manoeuvre in order to
- find the best solution balancing risk protection and innovation openness.

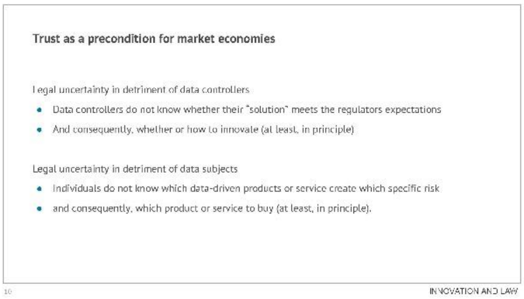
Examples in the CDPR:

- Principles of data processing (Art. 5)
- Responsibility principle (Art. 24)
- Privacy and security by design requirements (Art. 25 and 32)

8 INNOVATION AND LAW

Indeed, the result is high legal uncertainty.

9 INNOVATION AND LAW



Trust as a precondition for market economies

Legal uncertainty in detriment of data controllers

- Data controllers do not know whether their "solution" meets the regulators expectations
- And consequently, whether or how to innovate (at least, in principle)

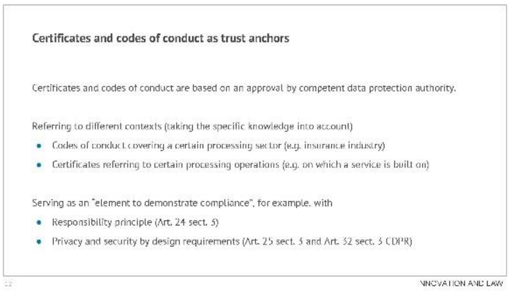
Legal uncertainty in detriment of data subjects

- Individuals do not know which data-driven products or service create which specific risk
- and consequently, which product or service to buy (at least, in principle).

10 INNOVATION AND LAW

How to solve the conflict between "openness to innovation" and legal uncertainty?

11 INNOVATION AND LAW



Certificates and codes of conduct as trust anchors

Certificates and codes of conduct are based on an approval by competent data protection authority.

Referring to different contexts (taking the specific knowledge into account)

- Codes of conduct covering a certain processing sector (e.g. insurance industry)
- Certificates referring to certain processing operations (e.g. on which a service is built on)

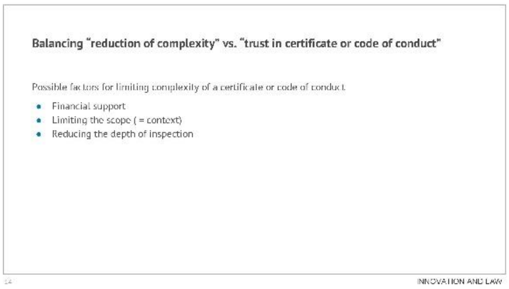
Serving as an "element to demonstrate compliance", for example, with

- Responsibility principle (Art. 24 sect. 3)
- Privacy and security by design requirements (Art. 25 sect. 3 and Art. 32 sect. 3 CDPR)

12 INNOVATION AND LAW

Last but not least:
How to take the "specific needs of micro-, small- and medium-sized enterprises" into account?

13 INNOVATION AND LAW

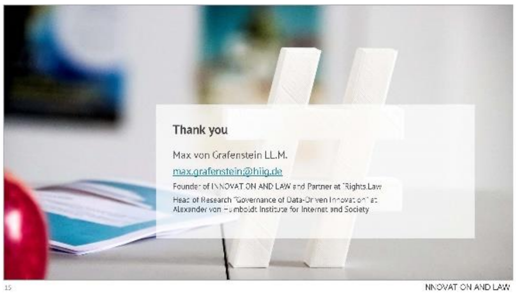


Balancing "reduction of complexity" vs. "trust in certificate or code of conduct"

Possible factors for limiting complexity of a certificate or code of conduct

- Financial support
- Limiting the scope (= context)
- Reducing the depth of inspection

14 INNOVATION AND LAW



Thank you

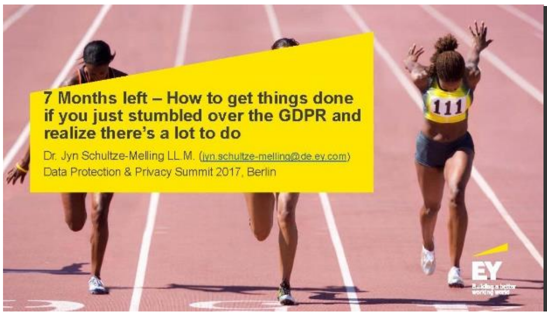
Max von Grafenstein LL.M.

max.grafenstein@hiig.de

Founder of INNOVATION AND LAW and Partner at iRights.Law

Head of Research "Governance of Data-Driven Innovation" at Alexander von Humboldt Institute for Internet and Society

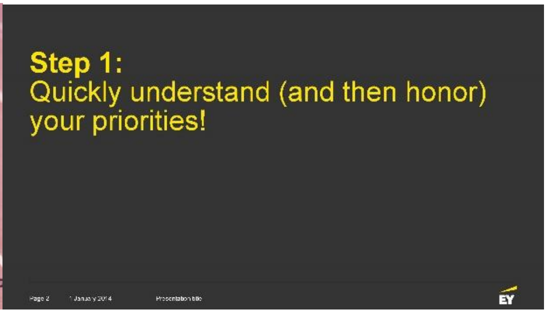
15 NNOVAT ON AND LAW



7 Months left – How to get things done if you just stumbled over the GDPR and realize there's a lot to do

Dr. Jyn Schultze-Melling LL.M. (jyn.schultze-melling@de.ey.com)
Data Protection & Privacy Summit 2017, Berlin

111
EY
Building a better working world

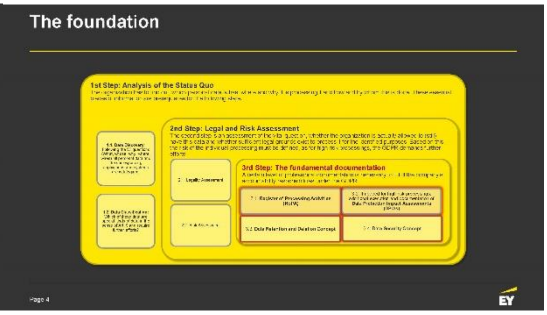


Step 1:
Quickly understand (and then honor) your priorities!

Page 2 1 January 2014 Presentation title

Is this you?

Page 3



The foundation

1st Step: Analysis of the Status Quo
The organization has to find out, which personal data it has, where and why it is processing it and how and by whom this is done. These essential pieces of information are prerequisites for the following steps.

1.1 Data Discovery: Following the W-questions (What, Where, Why, Where else, [illegible])

1.2 Data Classification: Which of these data are special categories of data [illegible] require further efforts?

2nd Step: Legal and Risk Assessment
The second step is an assessment of the vital question, whether the organization is actually allowed to hold/have this data and whether sufficient legal grounds exist to process it for the identified purposes. Based on this the risk of the individual processing must be defined, as for high risk processings, the GDPR demands further efforts.

2.1 Legality Assessment

2.2 Risk Assessment

3rd Step: The fundamental documentation
A certain level of professional documentation is necessary to fulfill the company's accountability responsibilities under the GDPR.

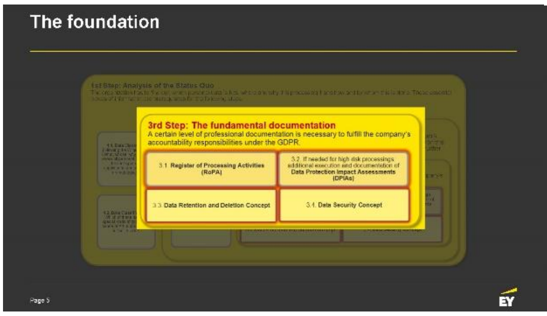
3.1 Register of Processing Activities (RoPA)

3.2 If needed for high risk processings additional execution and documentation of Data Protection Impact Assessments (DPIAs)

3.3 Data Retention and Deletion Concept

3.4 Data Security Concept

Page 4



The foundation

3rd Step: The fundamental documentation
A certain level of professional documentation is necessary to fulfill the company's accountability responsibilities under the GDPR.

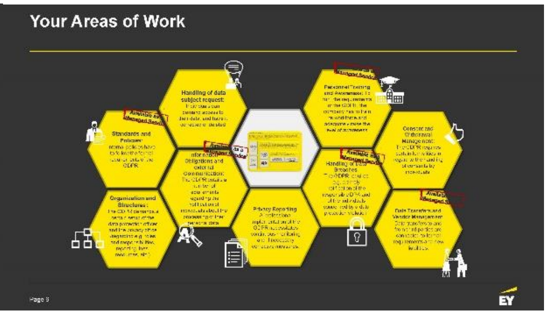
3.1 **Register of Processing Activities (RoPA)**

3.2 If needed for high risk processings additional execution and documentation of **Data Protection Impact Assessments (DPIAs)**

3.3 **Data Retention and Deletion Concept**

3.4 **Data Security Concept**

Page 5



Your Areas of Work

Standards and Policies: Internal policies have to follow the formal requirements of the GDPR

Handling of data subject request: Individuals can demand access to their data, and have it corrected or deleted

Information Obligations and external Communication: The GDPR entails a number of requirements regarding the notification of individuals about the processing of their personal data

Organization and Structures: The GDPR demands a certain setup of the data protection officer and the privacy office (regarding e.g. roles and responsibilities, reporting lines, resources, etc.)

Privacy Reporting: A professional implementation of the GDPR necessitates continuous monitoring and if necessary corrective measures.

Personnel Training and Awareness: To fulfil the requirements of the GDPR, the company has to train its workforce and adequately raise the level of awareness.

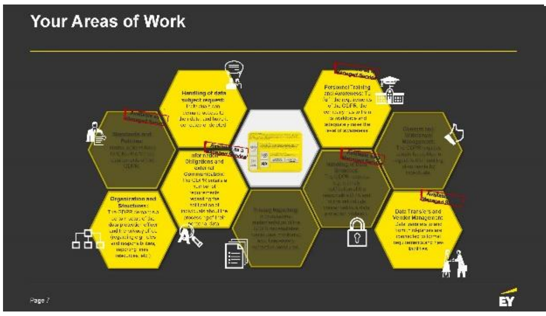
Handling of Data Breaches: The GDPR requires appropriately notification of the responsible DPA and of the individuals concerned by a data protection violation.

Consent and Withdrawal Management: The GDPR requires certain formalities in regard to the handling of consents by individuals

Data Transfers and Vendor Management: Data transfers to and from third parties are connected to formal requirements and new liabilities.

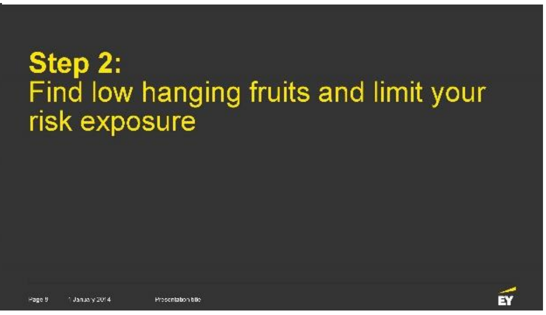
Available as Managed Service
Available as a Managed Service
Available as Managed Service
Available as Managed Service
Available as Managed Service

Page 9

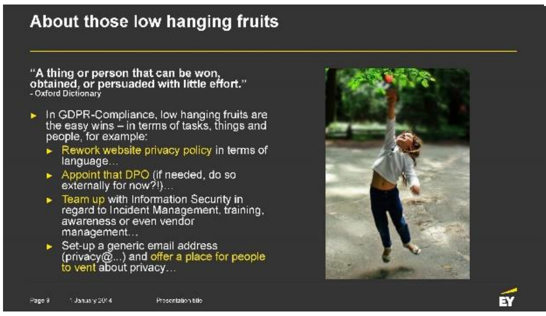


Your Areas of Work

Handling of data subject request:
Personnel Training and Awareness:
Standards and Policies:
Information Obligations and external Communication:
Contracts and Withdrawal Management:
Organization and Structures:
Privacy Reporting
Handling of Data Breaches
Data Transfers and Vendor Management:
Available as Managed Service



Step 2:
Find low hanging fruits and limit your risk exposure

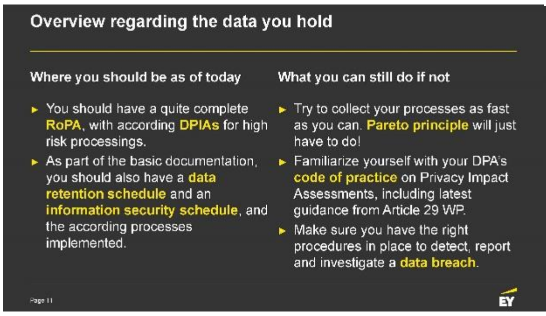


About those low hanging fruits

"A thing or person that can be won, obtained, or persuaded with little effort."
- Oxford Dictionary

- In GDPR-Compliance, low hanging fruits are the easy wins – in terms of tasks, things and people, for example:
  - Rework website privacy policy in terms of language…
  - Appoint that DPO (if needed, do so externally for now?!)…
  - Team up with Information Security in regard to Incident Management, training, awareness or even vendor management…
  - Set-up a generic email address (privacy@…) and offer a place for people to vent about privacy…

Step 3:
Pragmatic documentation



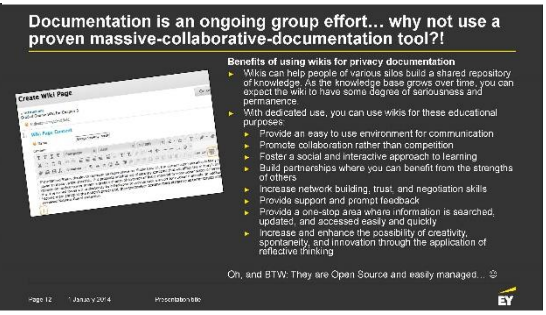
Overview regarding the data you hold

Where you should be as of today

- You should have a quite complete RoPA, with according DPIAs for high risk processings.
- As part of the basic documentation, you should also have a data retention schedule and an information security schedule, and the according processes implemented.

What you can still do if not

- Try to collect your processes as fast as you can. Pareto principle will just have to do!
- Familiarize yourself with your DPA's code of practice on Privacy Impact Assessments, including latest guidance from Article 29 WP.
- Make sure you have the right procedures in place to detect, report and investigate a data breach.



Documentation is an ongoing group effort… why not use a proven massive-collaborative-documentation tool?!

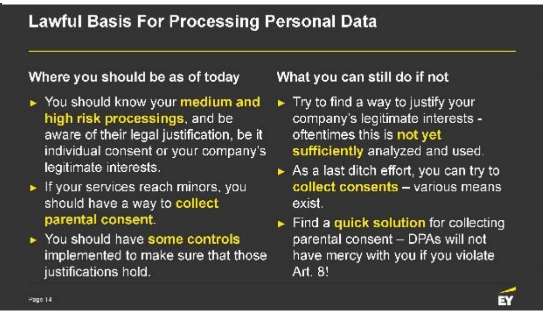
Create Wiki Page
Wiki Page Content

Benefits of using wikis for privacy documentation

- Wikis can help people of various silos build a shared repository of knowledge. As the knowledge base grows over time, you can expect the wiki to have some degree of seriousness and permanence.
- With dedicated use, you can use wikis for these educational purposes:
  - Provide an easy to use environment for communication
  - Promote collaboration rather than competition
  - Foster a social and interactive approach to learning
  - Build partnerships where you can benefit from the strengths of others
  - Increase network building, trust, and negotiation skills
  - Provide support and prompt feedback
  - Provide a one-stop area where information is searched, updated, and accessed easily and quickly
  - Increase and enhance the possibility of creativity, spontaneity, and innovation through the application of reflective thinking

Oh, and BTW: They are Open Source and easily managed… ☺

Step 4:
Effective Privacy Controls on a budget



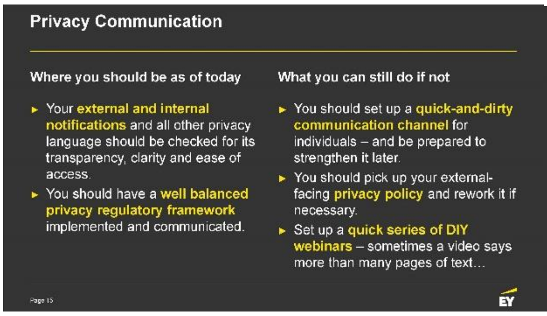
Lawful Basis For Processing Personal Data

Where you should be as of today

- You should know your medium and high risk processings, and be aware of their legal justification, be it individual consent or your company's legitimate interests.
- If your services reach minors, you should have a way to collect parental consent.
- You should have some controls implemented to make sure that those justifications hold.

What you can still do if not

- Try to find a way to justify your company's legitimate interests - oftentimes this is not yet sufficiently analyzed and used.
- As a last ditch effort, you can try to collect consents – various means exist.
- Find a quick solution for collecting parental consent – DPAs will not have mercy with you if you violate Art. 8!



Privacy Communication

Where you should be as of today

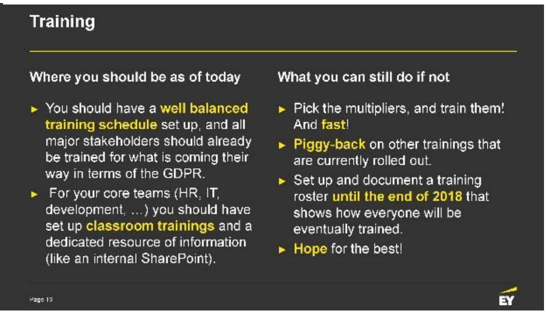
- Your **external and internal notifications** and all other privacy language should be checked for its transparency, clarity and ease of access.
- You should have a **well balanced privacy regulatory framework** implemented and communicated.

What you can still do if not

- You should set up a **quick-and-dirty communication channel** for individuals – and be prepared to strengthen it later.
- You should pick up your external-facing **privacy policy** and rework it if necessary.
- Set up a **quick series of DIY webinars** – sometimes a video says more than many pages of text…

Page 15

EY



Training

Where you should be as of today

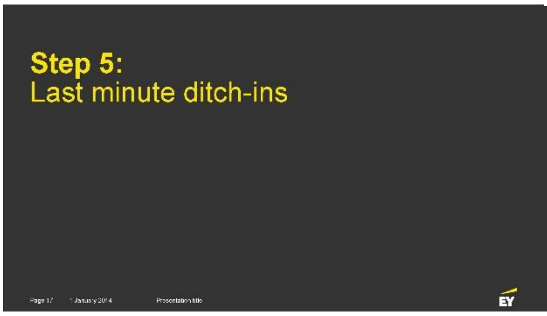
- You should have a **well balanced training schedule** set up, and all major stakeholders should already be trained for what is coming their way in terms of the GDPR.
- For your core teams (HR, IT, development, …) you should have set up **classroom trainings** and a dedicated resource of information (like an internal SharePoint).

What you can still do if not

- Pick the multipliers, and train them! And **fast**!
- **Piggy-back** on other trainings that are currently rolled out.
- Set up and document a training roster **until the end of 2018** that shows how everyone will be eventually trained.
- **Hope** for the best!

Page 16

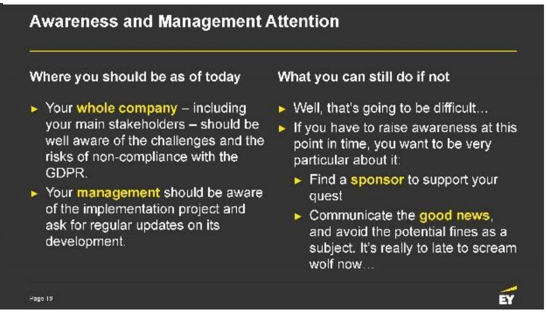
EY



Step 5:
Last minute ditch-ins

Page 17 1 January 2014 Presentation title

EY



Awareness and Management Attention

Where you should be as of today

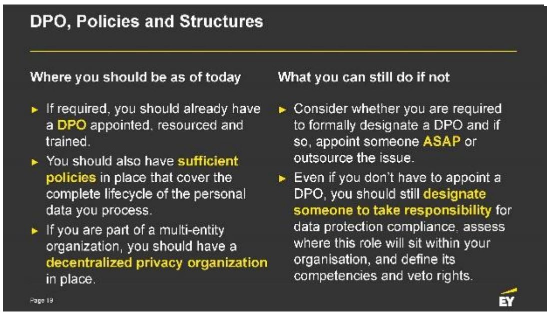
- Your **whole company** – including your main stakeholders – should be well aware of the challenges and the risks of non-compliance with the GDPR.
- Your **management** should be aware of the implementation project and ask for regular updates on its development.

What you can still do if not

- Well, that's going to be difficult…
- If you have to raise awareness at this point in time, you want to be very particular about it:
  - Find a **sponsor** to support your quest
  - Communicate the **good news**, and avoid the potential fines as a subject. It's really to late to scream wolf now…

Page 18

EY



DPO, Policies and Structures

Where you should be as of today

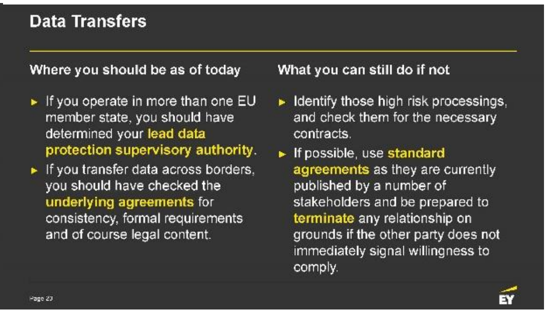
- If required, you should already have a **DPO** appointed, resourced and trained.
- You should also have **sufficient policies** in place that cover the complete lifecycle of the personal data you process.
- If you are part of a multi-entity organization, you should have a **decentralized privacy organization** in place.

What you can still do if not

- Consider whether you are required to formally designate a DPO and if so, appoint someone **ASAP** or outsource the issue.
- Even if you don't have to appoint a DPO, you should still **designate someone to take responsibility** for data protection compliance, assess where this role will sit within your organisation, and define its competencies and veto rights.

Page 19

EY



Data Transfers

Where you should be as of today

- If you operate in more than one EU member state, you should have determined your **lead data protection supervisory authority**.
- If you transfer data across borders, you should have checked the **underlying agreements** for consistency, formal requirements and of course legal content.

What you can still do if not

- Identify those high risk processings, and check them for the necessary contracts.
- If possible, use **standard agreements** as they are currently published by a number of stakeholders and be prepared to **terminate** any relationship on grounds if the other party does not immediately signal willingness to comply.

Page 20

EY

Thanks! Questions?

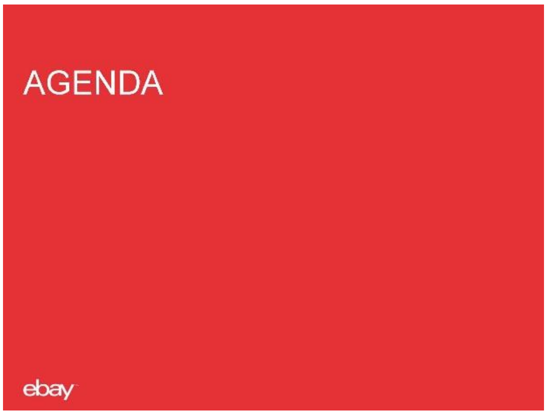
Page 21

EY

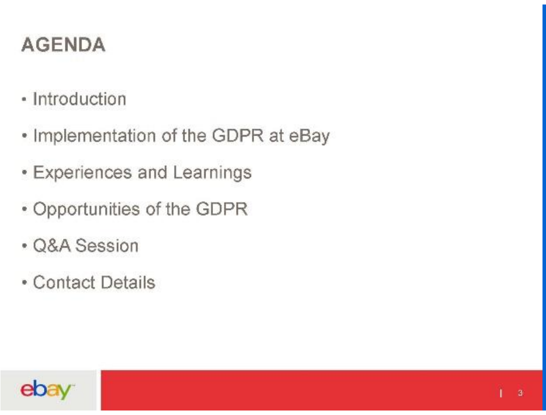
IMPLEMENTING THE GDPR & LEVERAGING PRIVACY AS A COMPETITIVE ADVANTAGE

Dr. Anna Zeiter, LL.M., Director of Privacy & Data Protection Officer, EMEA

Privacy & Data Protection Summit, 16 November 2017



AGENDA

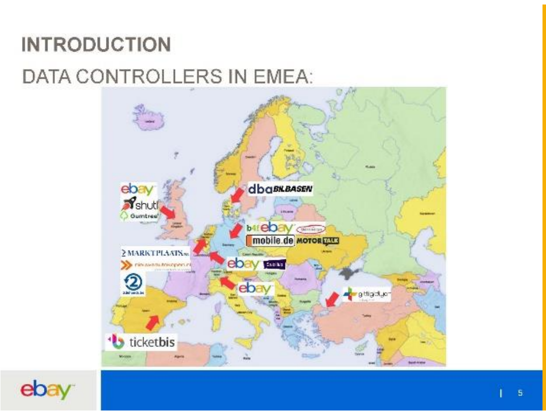


AGENDA

- Introduction
- Implementation of the GDPR at eBay
- Experiences and Learnings
- Opportunities of the GDPR
- Q&A Session
- Contact Details

| 3

INTRODUCTION

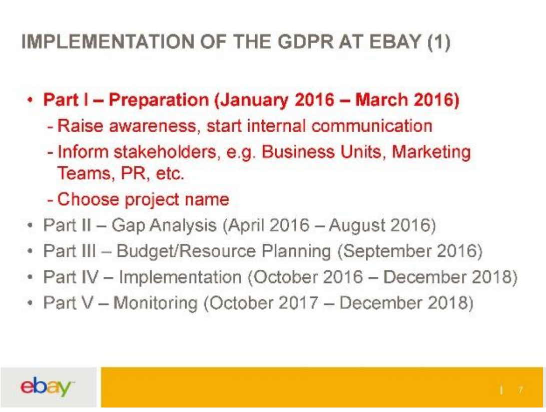


INTRODUCTION

DATA CONTROLLERS IN EMEA:

| 5

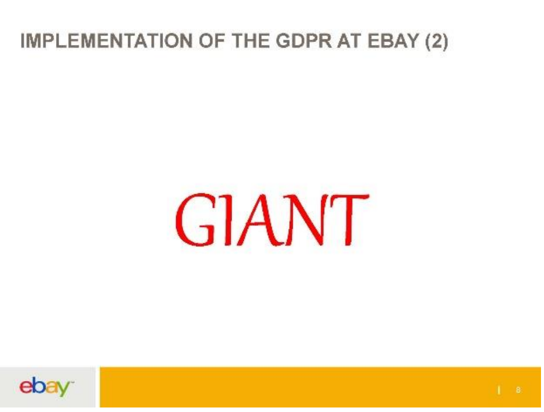
IMPLEMENTATION OF THE GDPR AT EBAY



IMPLEMENTATION OF THE GDPR AT EBAY (1)

- **Part I – Preparation (January 2016 – March 2016)**
  - Raise awareness, start internal communication
  - Inform stakeholders, e.g. Business Units, Marketing Teams, PR, etc.
  - Choose project name
- Part II – Gap Analysis (April 2016 – August 2016)
- Part III – Budget/Resource Planning (September 2016)
- Part IV – Implementation (October 2016 – December 2018)
- Part V – Monitoring (October 2017 – December 2018)

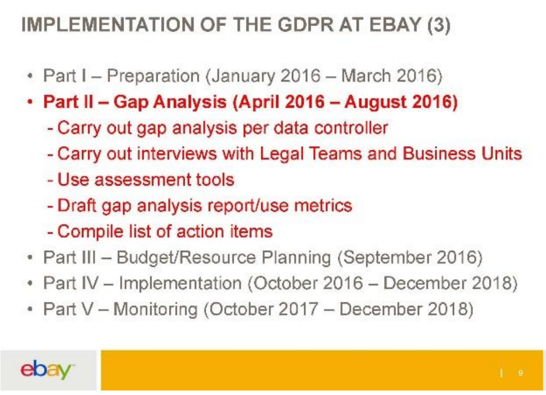
| 7



IMPLEMENTATION OF THE GDPR AT EBAY (2)

GIANT

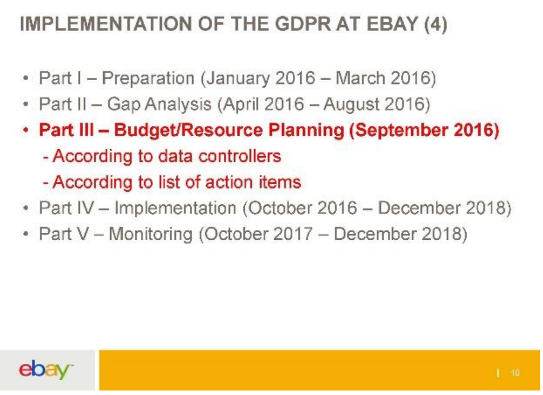
| 8



IMPLEMENTATION OF THE GDPR AT EBAY (3)

- Part I – Preparation (January 2016 – March 2016)
- **Part II – Gap Analysis (April 2016 – August 2016)**
  - Carry out gap analysis per data controller
  - Carry out interviews with Legal Teams and Business Units
  - Use assessment tools
  - Draft gap analysis report/use metrics
  - Compile list of action items
- Part III – Budget/Resource Planning (September 2016)
- Part IV – Implementation (October 2016 – December 2018)
- Part V – Monitoring (October 2017 – December 2018)

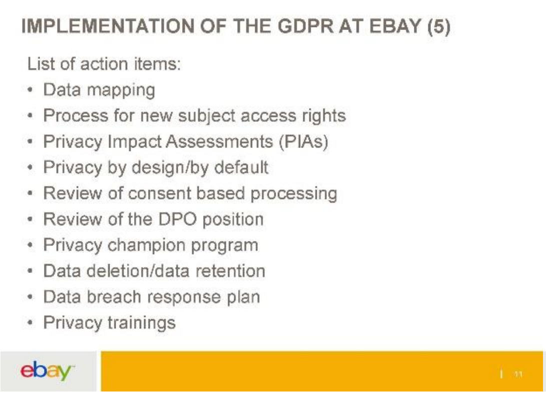
| 9



IMPLEMENTATION OF THE GDPR AT EBAY (4)

- Part I – Preparation (January 2016 – March 2016)
- Part II – Gap Analysis (April 2016 – August 2016)
- **Part III – Budget/Resource Planning (September 2016)**
  - According to data controllers
  - According to list of action items
- Part IV – Implementation (October 2016 – December 2018)
- Part V – Monitoring (October 2017 – December 2018)

| 10

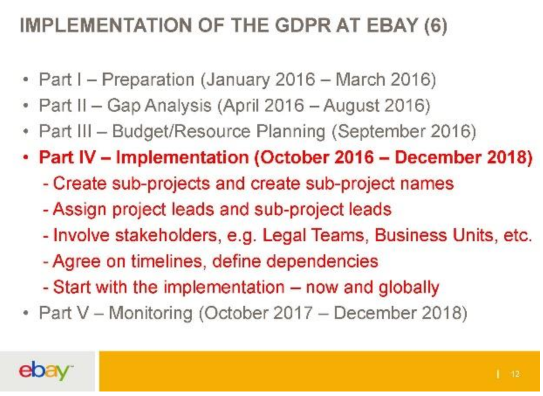


IMPLEMENTATION OF THE GDPR AT EBAY (5)

List of action items:

- Data mapping
- Process for new subject access rights
- Privacy Impact Assessments (PIAs)
- Privacy by design/by default
- Review of consent based processing
- Review of the DPO position
- Privacy champion program
- Data deletion/data retention
- Data breach response plan
- Privacy trainings

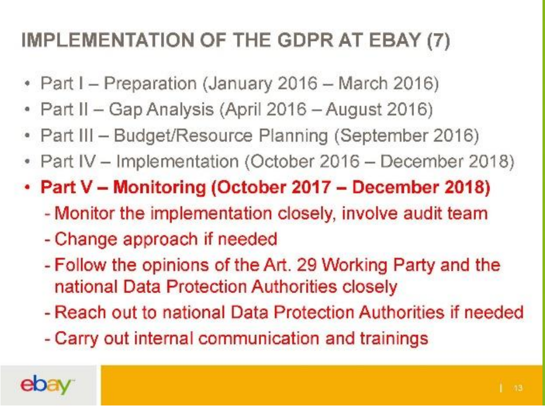
| 11



IMPLEMENTATION OF THE GDPR AT EBAY (6)

- Part I – Preparation (January 2016 – March 2016)
- Part II – Gap Analysis (April 2016 – August 2016)
- Part III – Budget/Resource Planning (September 2016)
- **Part IV – Implementation (October 2016 – December 2018)**
  - Create sub-projects and create sub-project names
  - Assign project leads and sub-project leads
  - Involve stakeholders, e.g. Legal Teams, Business Units, etc.
  - Agree on timelines, define dependencies
  - Start with the implementation – now and globally
- Part V – Monitoring (October 2017 – December 2018)

| 12

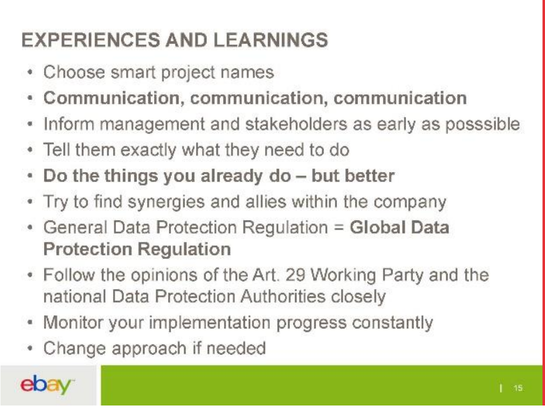


IMPLEMENTATION OF THE GDPR AT EBAY (7)

- Part I – Preparation (January 2016 – March 2016)
- Part II – Gap Analysis (April 2016 – August 2016)
- Part III – Budget/Resource Planning (September 2016)
- Part IV – Implementation (October 2016 – December 2018)
- **Part V – Monitoring (October 2017 – December 2018)**
  - Monitor the implementation closely, involve audit team
  - Change approach if needed
  - Follow the opinions of the Art. 29 Working Party and the national Data Protection Authorities closely
  - Reach out to national Data Protection Authorities if needed
  - Carry out internal communication and trainings

| 13

EXPERIENCES AND LEARNINGS

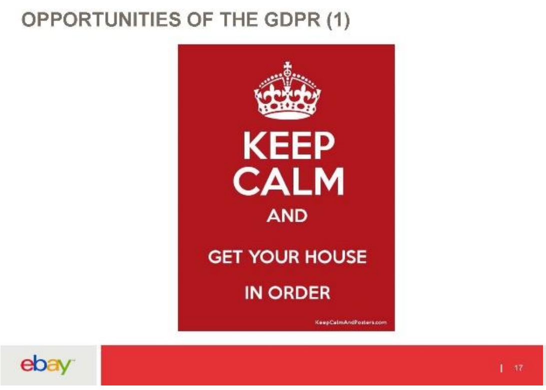


EXPERIENCES AND LEARNINGS

- Choose smart project names
- **Communication, communication, communication**
- Inform management and stakeholders as early as posssible
- Tell them exactly what they need to do
- **Do the things you already do – but better**
- Try to find synergies and allies within the company
- General Data Protection Regulation = **Global Data Protection Regulation**
- Follow the opinions of the Art. 29 Working Party and the national Data Protection Authorities closely
- Monitor your implementation progress constantly
- Change approach if needed

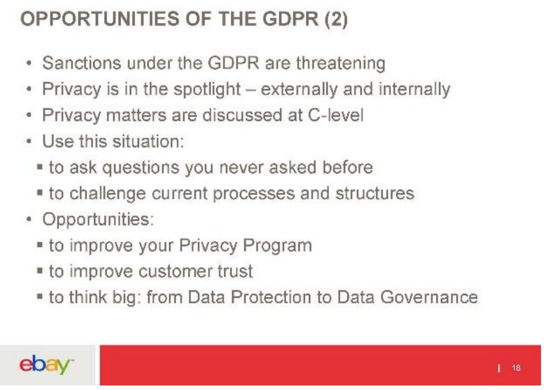
| 15

OPPRTUNITIES OF THE GDPR



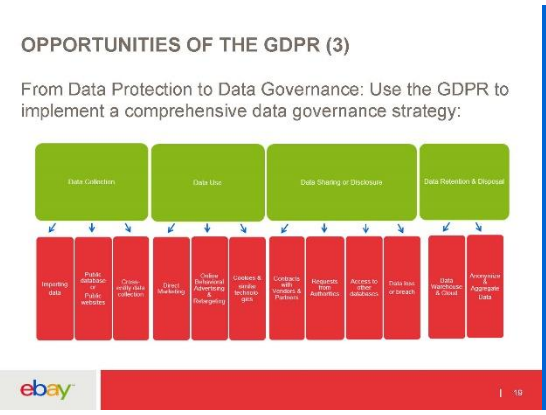
OPPORTUNITIES OF THE GDPR (1)

KEEP CALM AND GET YOUR HOUSE IN ORDER



OPPORTUNITIES OF THE GDPR (2)

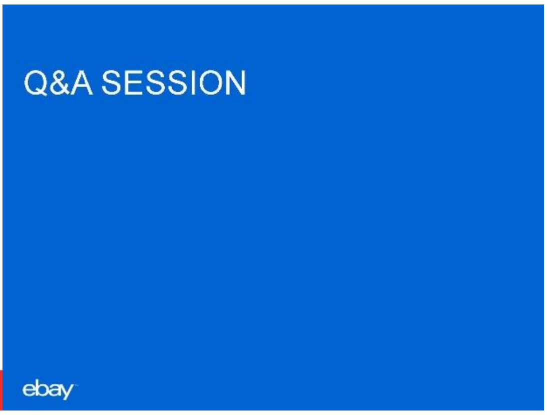
- Sanctions under the GDPR are threatening
- Privacy is in the spotlight – externally and internally
- Privacy matters are discussed at C-level
- Use this situation:
  - to ask questions you never asked before
  - to challenge current processes and structures
- Opportunities:
  - to improve your Privacy Program
  - to improve customer trust
  - to think big: from Data Protection to Data Governance



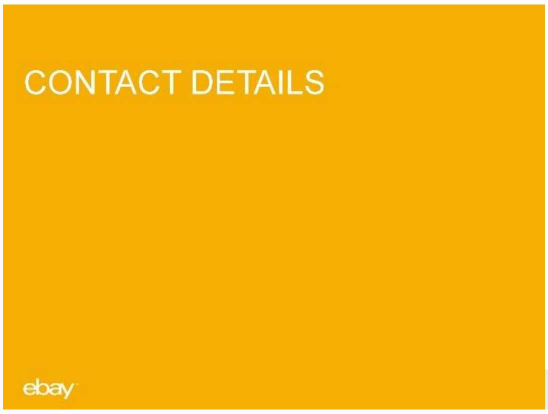
OPPORTUNITIES OF THE GDPR (3)

From Data Protection to Data Governance: Use the GDPR to implement a comprehensive data governance strategy:

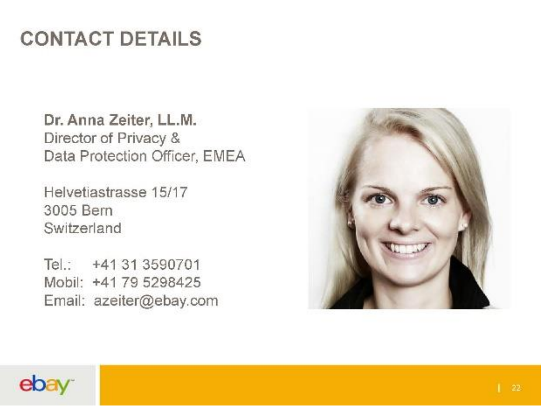
Data Collection
Data Use
Data Sharing or Disclosure
Data Retention & Disposal
Importing data
Public database or Public websites
Cross-entity data collection
Direct Marketing
Online Behavioral Advertising & Retargeting
Cookies & similar technologies
Contracts with Vendors & Partners
Requests from Authorities
Access to other databases
Data loss or breach
Data Warehouse & Cloud
Anonymize & Aggregate Data



Q&A SESSION



CONTACT DETAILS

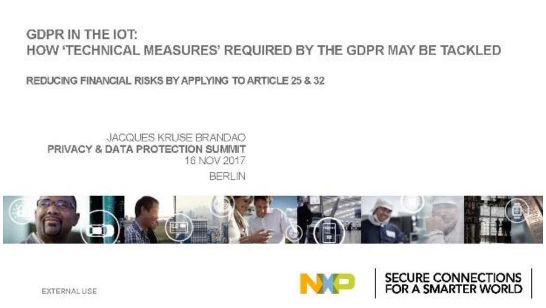


CONTACT DETAILS

Dr. Anna Zeiter, LL.M.
Director of Privacy &
Data Protection Officer, EMEA

Helvetiastrasse 15/17
3005 Bern
Switzerland

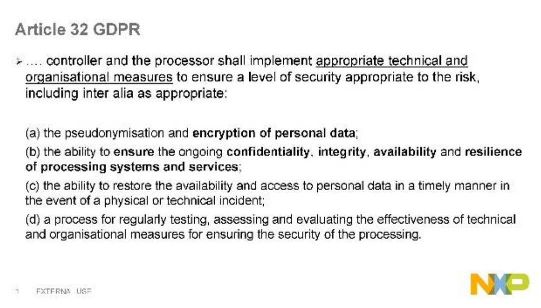
Tel.: +41 31 3590701
Mobil: +41 79 5298425
Email: azeiter@ebay.com



GDPR IN THE IOT:
HOW 'TECHNICAL MEASURES' REQUIRED BY THE GDPR MAY BE TACKLED

REDUCING FINANCIAL RISKS BY APPLYING TO ARTICLE 25 & 32

JACQUES KRUSE BRANDAO
PRIVACY & DATA PROTECTION SUMMIT
16 NOV 2017
BERLIN



Article 32 GDPR

➢ .... controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and **encryption of personal data**;
(b) the ability to **ensure** the ongoing **confidentiality**, **integrity**, **availability** and **resilience of processing systems and services**;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Article 25 GDPR

- Taking into account the state of the art, the cost of implementation and the nature, scope, (…) the controller shall, (…), implement appropriate technical and organisational measures, such as pseudonymisation, (…), such as data minimization, (…)

Problem (=challenges!)

1. What are appropriate technical measures?
2. What is “State-of-the-Art”?

- **Up to now there is no technical catalogue or guideline available what exactly needs to be implemented in terms of cybersecurity into IoT devices** which are processing (handling, using, storing, deleting, etc.) personal data to fulfil the GDPR requirements.
- Standards do **only exist for specific segments and use cases**.
- ‘State-of-the-art’ is dynamic.
- Fast innovation cycles make it difficult for standardization to be on time.
- “Security” is mentioned 50 x in GDPR text! But not defined in detail.

-> Anyway the message by the data protection authorities is clear: no privacy without security!

What do we need?

- Generate **Legal certainty** for investors by defining “certification of privacy”
- Enhance the **European** Cybersecurity Certification Framework by privacy requirements to fill the requirements of the GDPR, involving the EDPB and national data protection authorities
- “Impact”:
Generate **Risk+Impact Assessment** Framework, e.g. higher security levels for more sensitive data (e.g. patients file vs. fridge content)
- “State-of-the-Art”: **Generate Catalogue of key principles** for security and privacy, based on existing standards, e.g. privacy features in SMGW / Comms Hubs / etc.
- A **mapping of each key principle to existing standard(s) and certification schemes**
- Filling the gaps via ESO

Security in IoT / State of the Art (SOTA)

Law Firm *Arthur's Legal* has analyzed 27 SOTA Security Recommendations, Frameworks & Guidelines

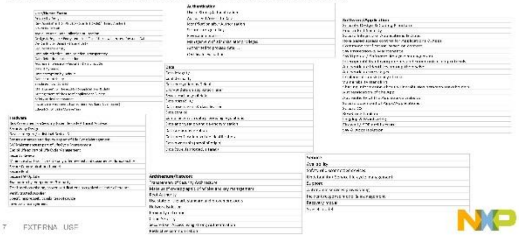
1. European Commission (EC) & Alliance for Internet of Things Innovation (AIOTI): Report on Workshop on Security & Privacy in IoT (2017)
2. Alliance for Internet of Things Innovation (AIOTI): Report on Workshop on Security and Privacy in the Hyper-Connected World (2016)
3. European Commission (EC): Best available techniques reference document for the cyber-security and privacy of the 10 minimum functional requirements of the Smart Metering Systems (2016)
4. European Union Agency for Network and Information Security (ENISA): Auditing Security Measures (2013)
5. European Union Agency for Network and Information Security (ENISA): Cloud Certification Schemes Metaframework (2014)
6. Energy Expert Cyber Security Platform: Cyber Security in the Energy Sector (2017)
7. HM Government, Department for Transport, Centre for the Protection of National Infrastructure: The Key Principles of Cyber Security for Connected and Automated Vehicles (2017)
8. Autorité de régulation des communications électroniques et des postes (ARCEP): Preparing for the Internet of things revolution (2016)
9. United States Department of Commerce (DoC): Fostering the advancement of the Internet of Things (2017)
10. United States Department of Homeland Security: Strategic Principles for Securing the Internet of Things (2016)
11. United States Department of Health and Human Services, Food and Drug Administration: Postmarket Management of Cybersecurity in Medical Devices (2016)
12. United States Department of Health and Human Services, Food and Drug Administration: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
13. United States Government Accountability Office: Technology Assessment: Internet of Things: Status and implications of an increasingly connected world (2017)
14. National Institute of Standards and Technology (NIST): Networks of Things (2016)
15. IoT Alliance Australia (IoTAA): Internet of Things Security Guideline (2017)
16. GSM Association (GSMA): IoT Security Guidelines Overview Document (2016)
17. GSM Association (GSMA): IoT Security Guidelines for Service Ecosystems (2016)
18. GSM Association (GSMA): IoT Security Guidelines for Endpoint Ecosystems (2016)
19. GSM Association (GSMA): IoT Security Guidelines for Network Operators (2016)
20. IoT Security Foundation (IoTSF): IoT Security Compliance Framework (2016)
21. IoT Security Foundation (IoTSF): Connected Consumer Products Best Practice Guidelines (2016)
22. IoT Security Foundation (IoTSF): Vulnerability Disclosure (2016)
23. Broadband Internet Technical Advisory Group (BITAG): Internet of Things (IoT) Security and Privacy Recommendations (2016)
24. International Organization for Standardization (ISO): Internet of Things Preliminary Report (2014)
25. The Center for Internet Security (CIS): Critical Security Controls (2016)
26. Internet Society: Global Internet Report 2016 (2016)
27. [illegible] Alliance: [illegible] Cyber Hygiene (2016)

What can we do in the meanwhile?

- Fill the time gap by **applying to Key Principles & Means** when it comes to Security & Privacy covering
  - User/Human Factor
  - Data
  - Service
  - Software/Application
  - Hardware
  - Authentication
  - Infrastructure/Network

Segmentation of Key Principles & Means

70+ Security Requirements & Principles could be derived from that exercise, e.g. end-to-end security, secure boot, secure storage of keys (see back-up)



Next Steps to prepare for the GDPR

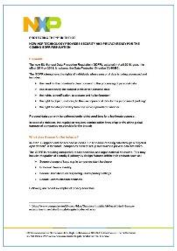
1. Protect PII in the IoT devices and services by mentioned Key Principles & Means.
2. Ask the local Data Protection Authority how to comply for the GDPR.
3. Apply for certification of IoT devices and services to receive approval for ‚GDPR-compliance‘.

-> As NXP we will support you in the implementation of security features into IoT devices and services.

-> Additionally we support the discussion with the authorities and the certification process.

How NXP Technology provides Security and Privacy ready for the coming GDPR Regulation

- PROTECTING THE “I” IN THE IOT

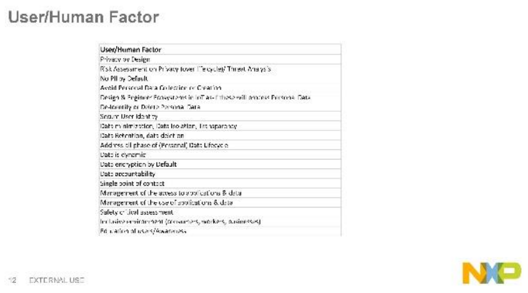


Thank you for listening!

SECURE CONNECTIONS
FOR A SMARTER WORLD

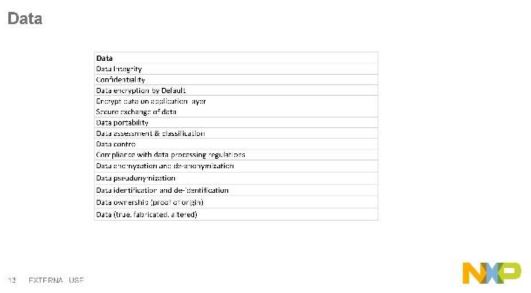
Jacques Kruse Brandao
jacques-kruse-brandao@nxp.com

BACK-UP


User/Human Factor

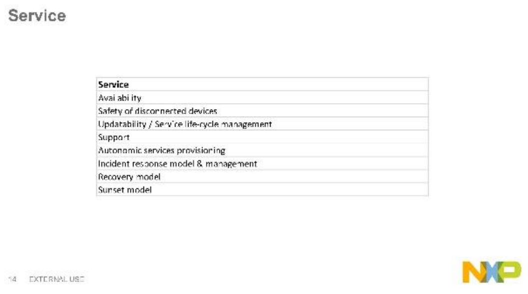
User/Human Factor
Privacy by Design
Risk Assessment on Privacy (over lifecycle)/ Threat Analysis No PII by Default Avoid Personal Data Collection or Creation Design & Engineer Ecosystems in IoT as if these will process Personal Data De-identify or Delete Personal Data
Secure User Identity
Data minimization, Data Isolation, Transparency
Data Retention, data deletion
Address all phase of (Personal) Data Lifecycle
Data is dynamic
Data encryption by Default
Data accountability
Single point of contact
Management of the access to applications & data
Management of the use of applications & data
Safety critical assessment Inclusive environment (consumers, workers, businesses) Education of users/Awareness

12 EXTERNAL USE


Data

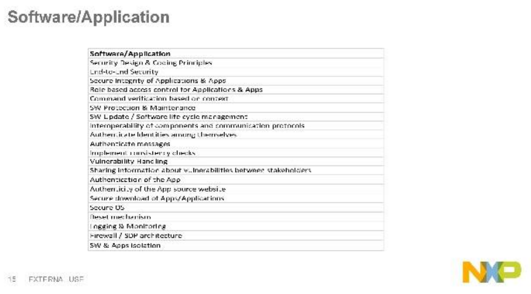
Data
Data Integrity
Confidentiality
Data encryption by Default
Encrypt data on application layer Secure exchange of data
Data portability
Data assessment & classification
Data control
Compliance with data processing regulations
Data anonymization and de-anonymization
Data pseudonymization
Data identification and de-identification
Data ownership (proof of origin)
Data (true, fabricated, altered)

13 EXTERNAL USE


Service

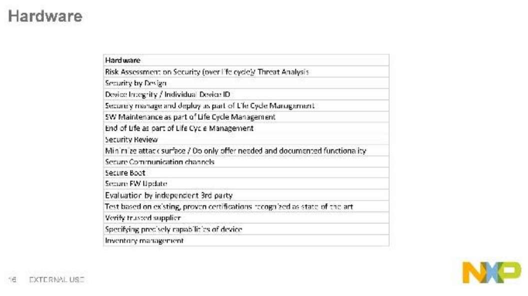
Service
Availability
Safety of disconnected devices
Updatability / Service life-cycle management
Support
Autonomic services provisioning
Incident response model & management
Recovery model
Sunset model

14 EXTERNAL USE


Software/Application

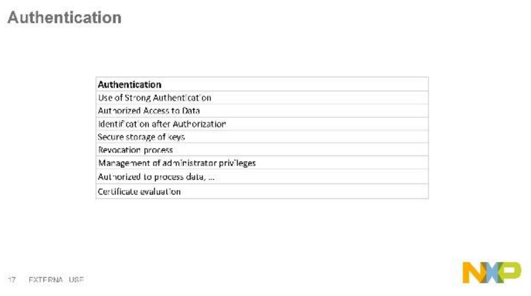
Software/Application
Security Design & Coding Principles End-to-End Security
Secure Integrity of Applications & Apps
Role based access control for Applications & Apps
Command verification based on context
SW Protection & Maintenance
SW Update / Software life cycle management
Interoperability of components and communication protocols
Authenticate Identities among themselves
Authenticate messages
Implement consistency checks
Vulnerability Handling
Sharing information about vulnerabilities between stakeholders
Authentication of the App
Authenticity of the App source website Secure download of Apps/Applications
Secure OS
Reset mechanism
Logging & Monitoring
Firewall / SDP architecture
SW & Apps isolation

15 EXTERNAL USE


Hardware

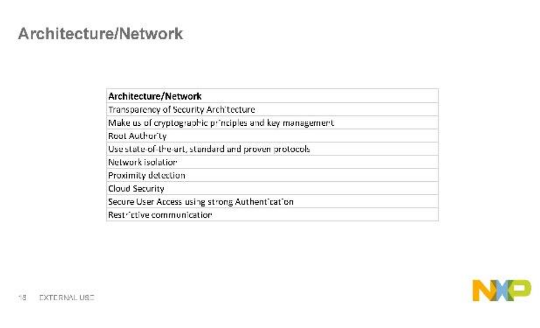
Hardware
Risk Assessment on Security (over life cycle)/ Threat Analysis
Security by Design
Device Integrity / Individual Device ID
Securely manage and deploy as part of Life Cycle Management
SW Maintenance as part of Life Cycle Management
End of Life as part of Life Cycle Management Security Review
Minimize attack surface / Do only offer needed and documented functionality
Secure Communication channels
Secure Boot
Secure FW Update
Evaluation by independent 3rd party
Test based on existing, proven certifications recognized as state of the art
Verify trusted supplier
Specifying precisely capabilities of device
Inventory management

16 EXTERNAL USE


Authentication

Authentication
Use of Strong Authentication
Authorized Access to Data
Identification after Authorization
Secure storage of keys
Revocation process
Management of administrator privileges
Authorized to process data, ...
Certificate evaluation

17 EXTERNAL USE



Architecture/Network

Architecture/Network
Transparency of Security Arch'tecture
Make us of cryptographic pr'nciples and key managemert
Root Author'ty
Use state-of-the-art, standard and proven protocols
Network isolatior
Proximity detection
Cloud Security
Secure User Access using strong Authent'cat'on
Rest'ictive communicatior

18 EXTERNAL USE

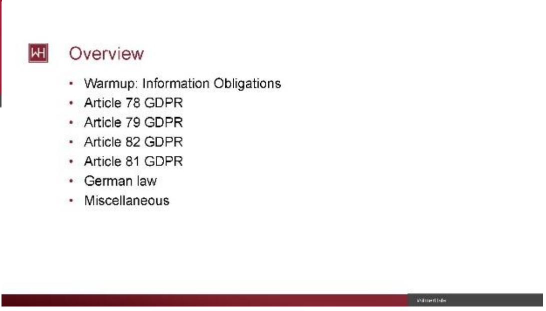
SECURE CONNECTIONS
FOR A SMARTER WORLD

Preparing for Litigation under the GDPR – The Companies' Perspective

Dr. Martin Braun

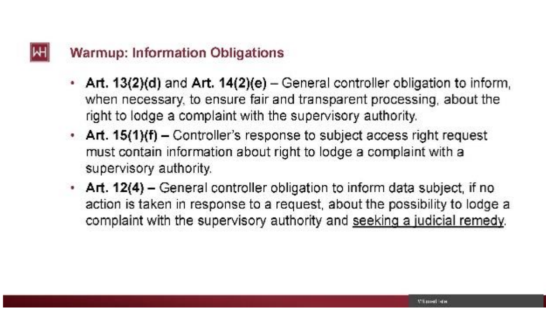
Privacy & Data Protection Summit
Berlin, 16-17 November 2017

WILMERHALE®



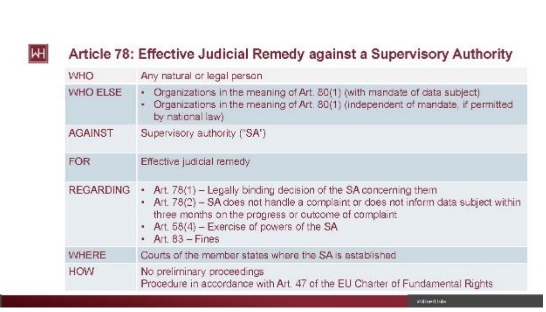
Overview

- Warmup: Information Obligations
- Article 78 GDPR
- Article 79 GDPR
- Article 82 GDPR
- Article 81 GDPR
- German law
- Miscellaneous



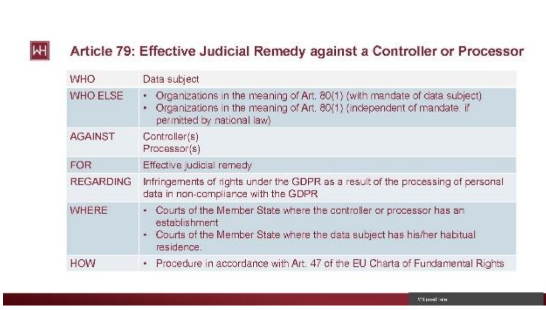
Warmup: Information Obligations

- **Art. 13(2)(d)** and **Art. 14(2)(e)** – General controller obligation to inform, when necessary, to ensure fair and transparent processing, about the right to lodge a complaint with the supervisory authority.
- **Art. 15(1)(f) –** Controller's response to subject access right request must contain information about right to lodge a complaint with a supervisory authority.
- **Art. 12(4) –** General controller obligation to inform data subject, if no action is taken in response to a request, about the possibility to lodge a complaint with the supervisory authority and seeking a judicial remedy.



Article 78: Effective Judicial Remedy against a Supervisory Authority

WHO	Any natural or legal person
WHO ELSE	• Organizations in the meaning of Art. 80(1) (with mandate of data subject) • Organizations in the meaning of Art. 80(1) (independent of mandate, if permitted by national law)
AGAINST	Supervisory authority ("SA")
FOR	Effective judicial remedy
REGARDING	• Art. 78(1) – Legally binding decision of the SA concerning them • Art. 78(2) – SA does not handle a complaint or does not inform data subject within three months on the progress or outcome of complaint • Art. 58(4) – Exercise of powers of the SA • Art. 83 – Fines
WHERE	Courts of the member states where the SA is established
HOW	No preliminary proceedings Procedure in accordance with Art. 47 of the EU Charter of Fundamental Rights

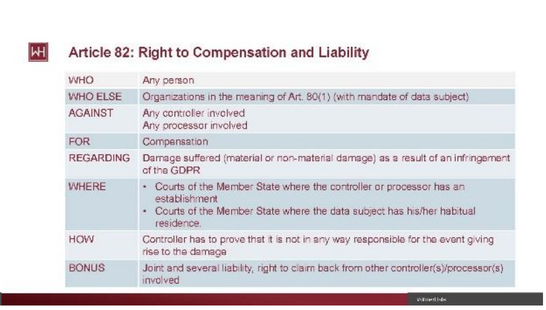


Article 79: Effective Judicial Remedy against a Controller or Processor

WHO	Data subject
WHO ELSE	• Organizations in the meaning of Art. 80(1) (with mandate of data subject) • Organizations in the meaning of Art. 80(1) (independent of mandate. if permitted by national law)

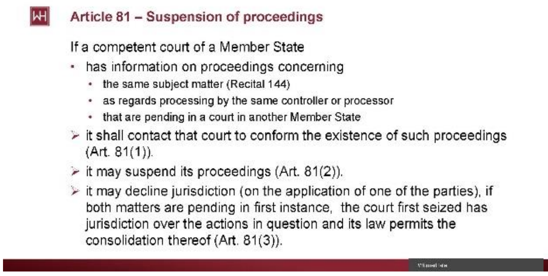
AGAINST	Controller(s)
	Processor(s)

FOR	Effective judicial remedy
REGARDING	Infringements of rights under the GDPR as a result of the processing of personal data in non-compliance with the GDPR
WHERE	• Courts of the Member State where the controller or processor has an establishment • Courts of the Member State where the data subject has his/her habitual residence.
HOW	• Procedure in accordance with Art. 47 of the EU Charta of Fundamental Rights



Article 82: Right to Compensation and Liability

WHO	Any person
WHO ELSE	Organizations in the meaning of Art. 80(1) (with mandate of data subject)
AGAINST	Any controller involved Any processor involved
FOR	Compensation
REGARDING	Damage suffered (material or non-material damage) as a result of an infringement of the GDPR
WHERE	• Courts of the Member State where the controller or processor has an establishment • Courts of the Member State where the data subject has his/her habitual residence.
HOW	Controller has to prove that it is not in any way responsible for the event giving rise to the damage
BONUS	Joint and several liability, right to claim back from other controller(s)/processor(s) involved



Article 81 – Suspension of proceedings

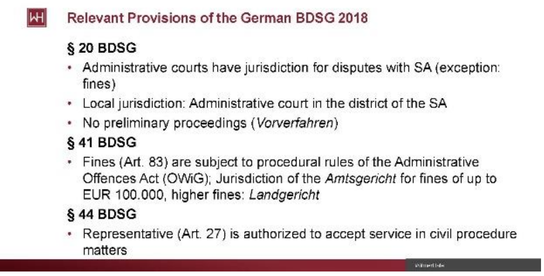
If a competent court of a Member State

- has information on proceedings concerning
  - the same subject matter (Recital 144)
  - as regards processing by the same controller or processor
  - that are pending in a court in another Member State

➢ it shall contact that court to conform the existence of such proceedings (Art. 81(1)).

➢ it may suspend its proceedings (Art. 81(2)).

➢ it may decline jurisdiction (on the application of one of the parties), if both matters are pending in first instance, the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof (Art. 81(3)).



Relevant Provisions of the German BDSG 2018

§ 20 BDSG

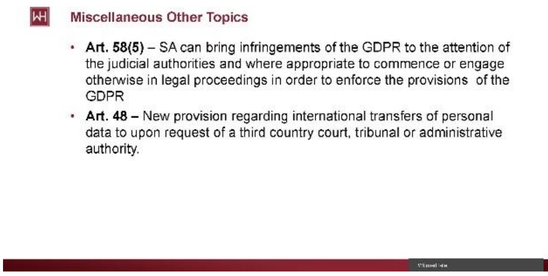
- Administrative courts have jurisdiction for disputes with SA (exception: fines)
- Local jurisdiction: Administrative court in the district of the SA
- No preliminary proceedings (*Vorverfahren*)

§ 41 BDSG

- Fines (Art. 83) are subject to procedural rules of the Administrative Offences Act (OWiG); Jurisdiction of the *Amtsgericht* for fines of up to EUR 100.000, higher fines: *Landgericht*

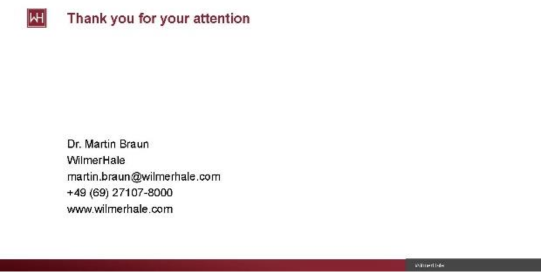
§ 44 BDSG

- Representative (Art. 27) is authorized to accept service in civil procedure matters



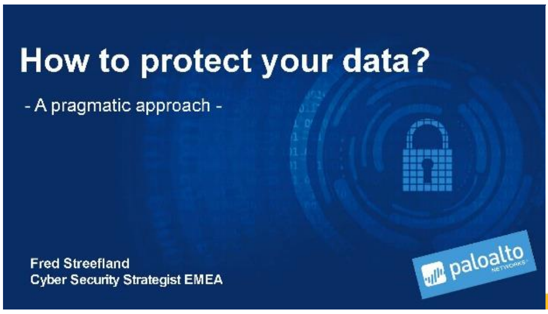
Miscellaneous Other Topics

- **Art. 58(5)** – SA can bring infringements of the GDPR to the attention of the judicial authorities and where appropriate to commence or engage otherwise in legal proceedings in order to enforce the provisions of the GDPR
- **Art. 48 –** New provision regarding international transfers of personal data to upon request of a third country court, tribunal or administrative authority.



Thank you for your attention

Dr. Martin Braun
WilmerHale
martin.braun@wilmerhale.com
+49 (69) 27107-8000
www.wilmerhale.com

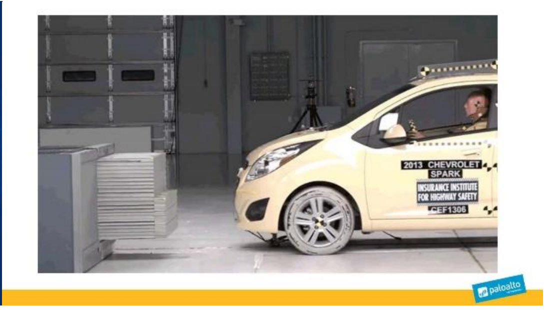


How to protect your data?

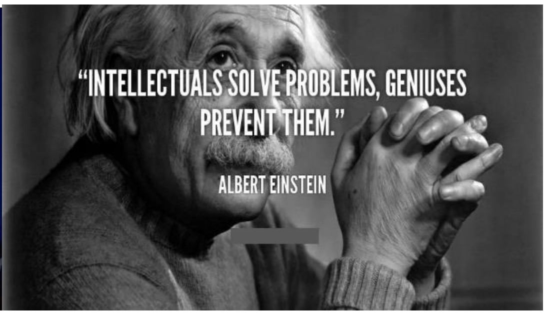
- A pragmatic approach -

Fred Streefland
Cyber Security Strategist EMEA

paloalto NETWORKS



INTRODUCTION (SPEAKER)



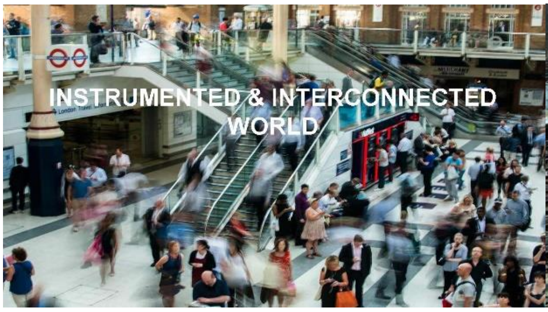
“INTELLECTUALS SOLVE PROBLEMS, GENIUSES PREVENT THEM.”

ALBERT EINSTEIN

TO PROTECT OUR WAY OF LIFE IN THE DIGITAL AGE BY PREVENTING SUCCESSFUL CYBER ATTACKS

- Our Mission -

SO WHAT'S THE PROBLEM?



INSTRUMENTED & INTERCONNECTED WORLD

COMPLEX ORGANIZATIONS

COMPLIANCY & REGULATIONS

DIVERSE, EVOLVING AND

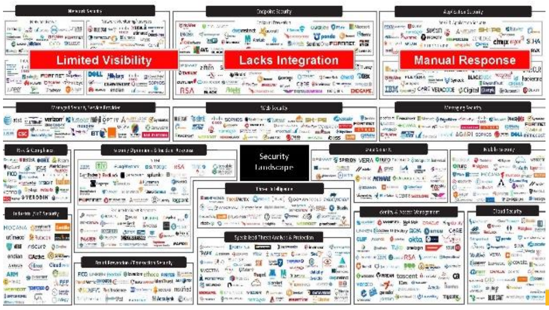
HIGHLY AUTOMATED ADVERSARIES

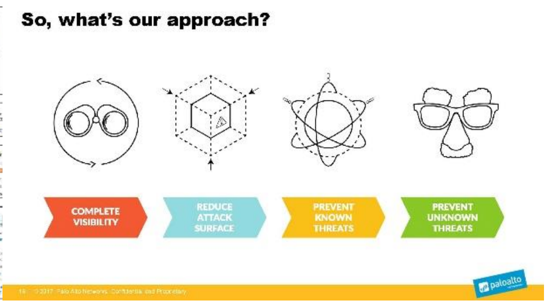
BUSINESS GROWTH

So, how can we handle these challenges...

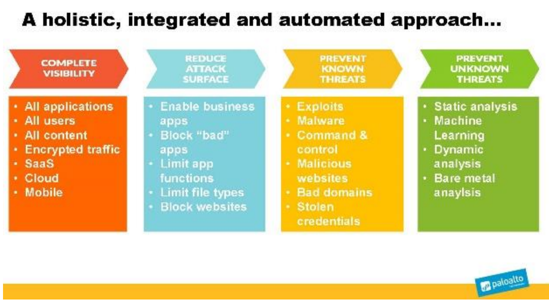
...and secure the organization?

CAN'T SEE THE WOODS FOR THE TREES



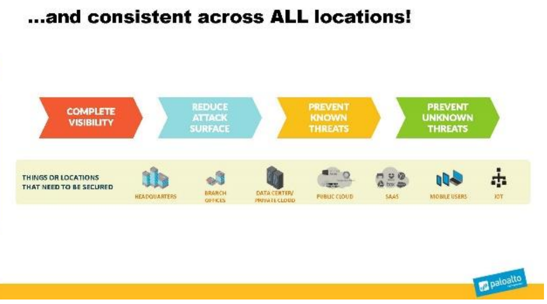


So, what's our approach?

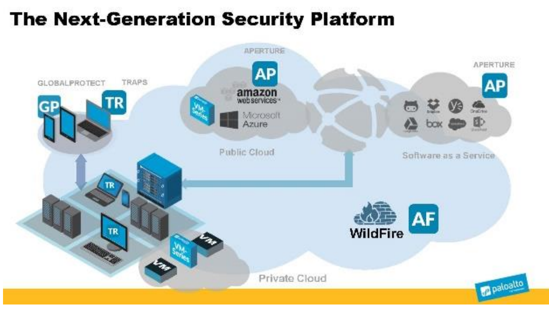


A holistic, integrated and automated approach…

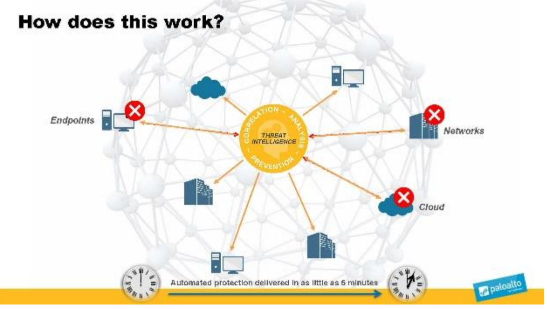
COMPLETE VISIBILITY	REDUCE ATTACK SURFACE	PREVENT KNOWN THREATS	PREVENT UNKNOWN THREATS
• All applications • All users • All content • Encrypted traffic • SaaS • Cloud • Mobile	• Enable business apps • Block "bad" apps • Limit app functions • Limit file types • Block websites	• Exploits • Malware • Command & control • Malicious websites • Bad domains • Stolen credentials	• Static analysis • Machine Learning • Dynamic analysis • Bare metal anaylsis



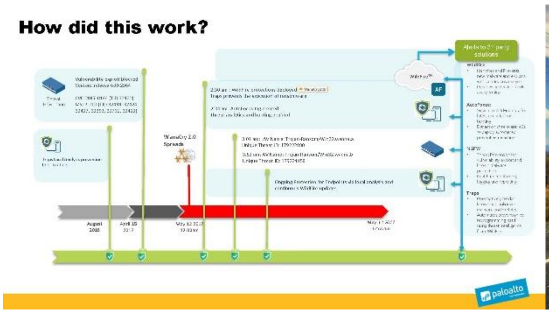
…and consistent across ALL locations!



The Next-Generation Security Platform



How does this work?

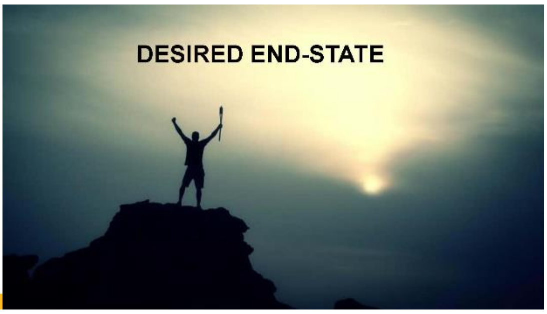


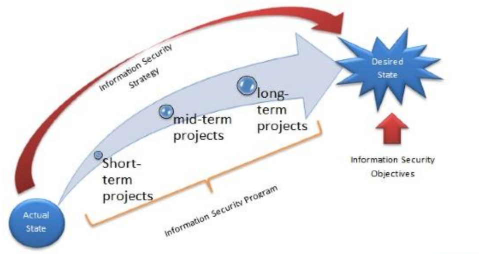
How did this work?

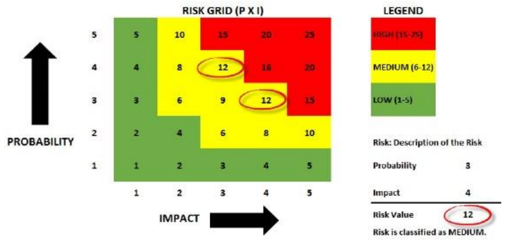
Alerts to 3rd party solutions
Vulnerability exploit blocked
WannaCry 2.0 Spreads
August 2016
April 15 2017
May 12 2017
WildFire
AF
AutoFocus
NGFW
Traps
Ongoing Protection for Endpoints via local analysis and continuous WildFire updates

Zero Trust design concept

- Focus on the business crown jewels (data)
- Design security from the Inside -> Out
  - Start with the assets or data that need protection
- Determine who or what needs access
  - Need to know/least-privilege
- Inspect and log all traffic




Information Security Strategy
Desired State
long-term projects
mid-term projects
Short-term projects
Actual State
Information Security Objectives
Information Security Program



RISK GRID (P X I)

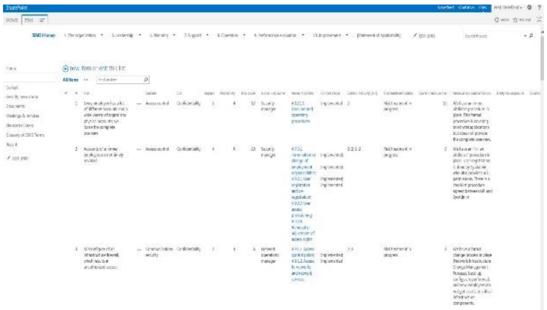
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5

LEGEND

- 🟥 HIGH (15-25)
- 🟨 MEDIUM (6-12)
- 🟩 LOW (1-5)

Risk: Description of the Risk	
Probability	3
Impact	4
Risk Value	12

Risk is classified as MEDIUM.



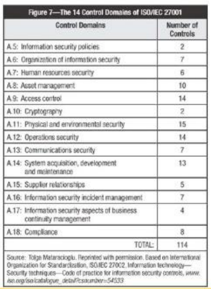
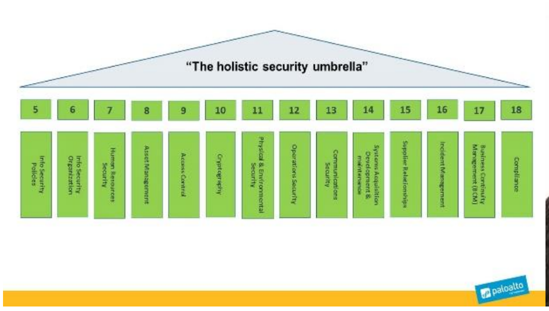
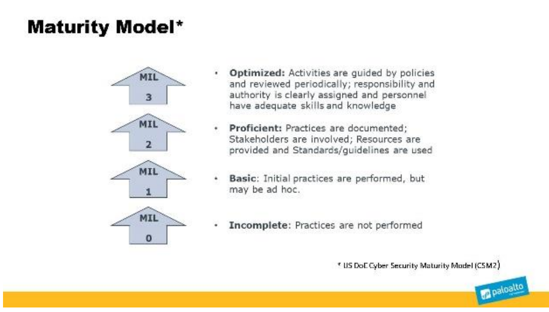


Figure 7—The 14 Control Domains of ISO/IEC 27001

Control Domains	Number of Controls
A.5: Information security policies	2
A.6: Organization of information security	7
A.7: Human resources security	6
A.8: Asset management	10
A.9: Access control	14
A.10: Cryptography	2
A.11: Physical and environmental security	15
A.12: Operations security	14
A.13: Communications security	7
A.14: System acquisition, development and maintenance	13
A.15: Supplier relationships	5
A.16: Information security incident management	7
A.17: Information security aspects of business continuity management	4
A.18: Compliance	8
TOTAL:	114

Source: Tolga Mataracioglu. Reprinted with permission. Based on International Organization for Standardization, ISO/IEC 27002, Information technology—Security techniques—Code of practice for information security controls, *www.iso.org/iso/catalogue_detail?csnumber=54533*





Maturity Model*

- **Optimized:** Activities are guided by policies and reviewed periodically; responsibility and authority is clearly assigned and personnel have adequate skills and knowledge
- **Proficient:** Practices are documented; Stakeholders are involved; Resources are provided and Standards/guidelines are used
- **Basic**: Initial practices are performed, but may be ad hoc.
- **Incomplete**: Practices are not performed

* US DoE Cyber Security Maturity Model (CSM2)

MIL 3
MIL 2
MIL 1
MIL 0
paloalto

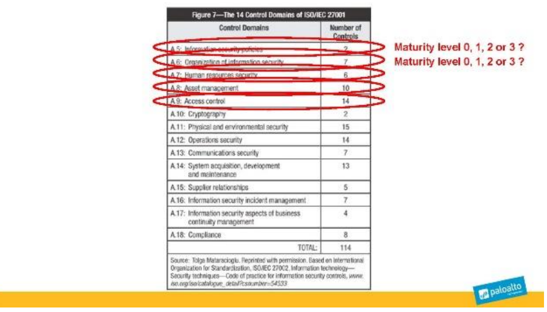


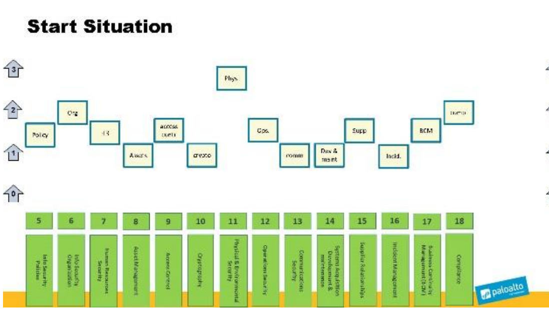
Figure 7—The 14 Control Domains of ISO/IEC 27001

Control Domains	Number of Controls
A.5: Information security policies	2
A.6: Organization of information security	7
A.7: Human resources security	6
A.8: Asset management	10
A.9: Access control	14
A.10: Cryptography	2
A.11: Physical and environmental security	15
A.12: Operations security	14
A.13: Communications security	7
A.14: System acquisition, development and maintenance	13
A.15: Supplier relationships	5
A.16: Information security incident management	7
A.17: Information security aspects of business continuity management	4
A.18: Compliance	8
TOTAL:	114

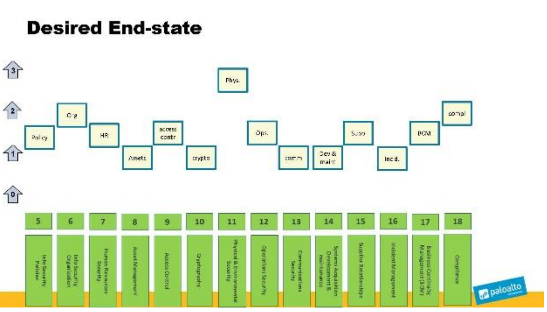
Source: Tolga Mataracioglu. Reprinted with permission. Based on International Organization for Standardization, ISO/IEC 27002, Information technology—Security techniques—Code of practice for information security controls, *www.iso.org/iso/catalogue_detail?csnumber=54533*

Maturity level 0, 1, 2 or 3 ?

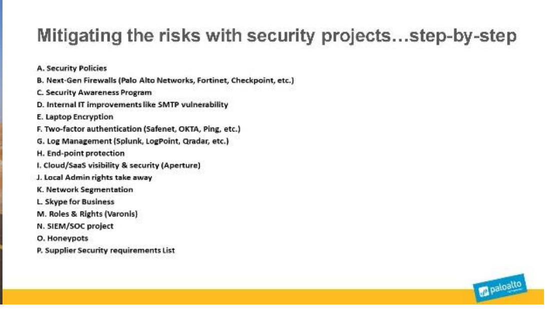
Maturity level 0, 1, 2 or 3 ?



Start Situation

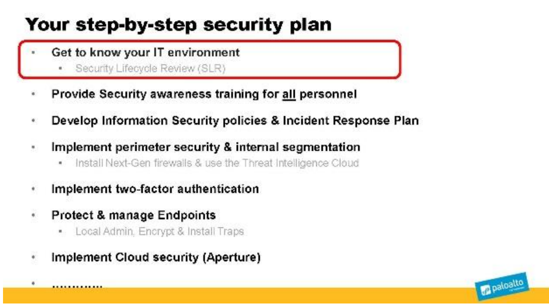


Desired End-state



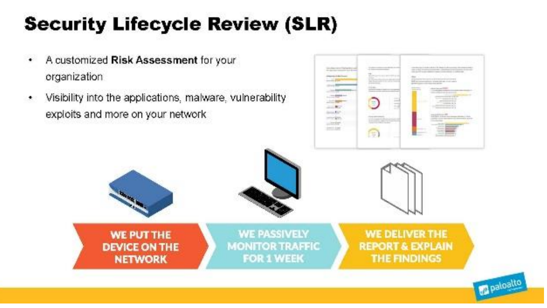
Mitigating the risks with security projects…step-by-step

A. Security Policies
B. Next-Gen Firewalls (Palo Alto Networks, Fortinet, Checkpoint, etc.)
C. Security Awareness Program
D. Internal IT improvements like SMTP vulnerability
E. Laptop Encryption
F. Two-factor authentication (Safenet, OKTA, Ping, etc.)
G. Log Management (Splunk, LogPoint, Qradar, etc.)
H. End-point protection
I. Cloud/SaaS visibility & security (Aperture)
J. Local Admin rights take away
K. Network Segmentation
L. Skype for Business
M. Roles & Rights (Varonis)
N. SIEM/SOC project
O. Honeypots
P. Supplier Security requirements List



Your step-by-step security plan

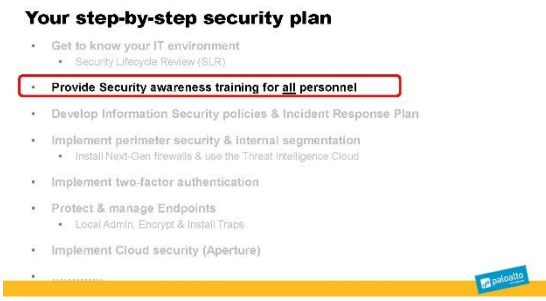
- Get to know your IT environment
  - Security Lifecycle Review (SLR)
- Provide Security awareness training for all personnel
- Develop Information Security policies & Incident Response Plan
- Implement perimeter security & internal segmentation
  - Install Next-Gen firewalls & use the Threat Intelligence Cloud
- Implement two-factor authentication
- Protect & manage Endpoints
  - Local Admin, Encrypt & Install Traps
- Implement Cloud security (Aperture)
- ………….



Security Lifecycle Review (SLR)

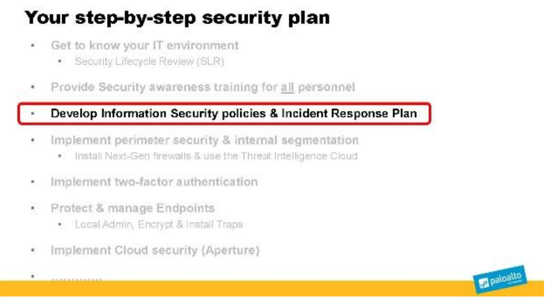
- A customized **Risk Assessment** for your organization
- Visibility into the applications, malware, vulnerability exploits and more on your network

WE PUT THE DEVICE ON THE NETWORK
WE PASSIVELY MONITOR TRAFFIC FOR 1 WEEK
WE DELIVER THE REPORT & EXPLAIN THE FINDINGS
paloalto



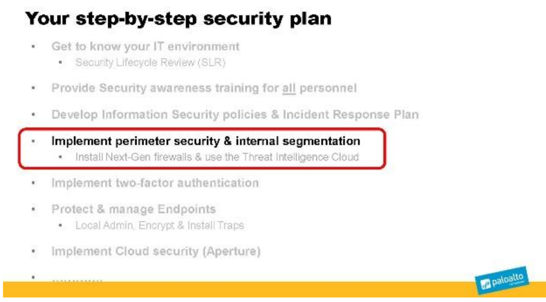
Your step-by-step security plan

- Get to know your IT environment
  - Security Lifecycle Review (SLR)
- **Provide Security awareness training for all personnel**
- Develop Information Security policies & Incident Response Plan
- Implement perimeter security & internal segmentation
  - Install Next-Gen firewalls & use the Threat Intelligence Cloud
- Implement two-factor authentication
- Protect & manage Endpoints
  - Local Admin, Encrypt & Install Traps
- Implement Cloud security (Aperture)
- ……………



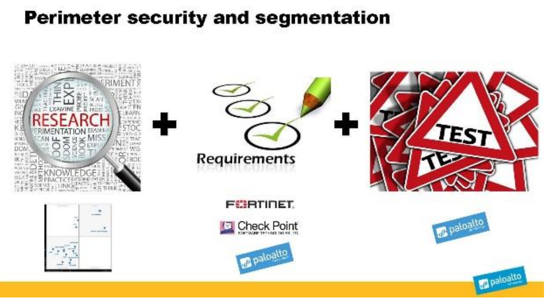
Your step-by-step security plan

- Get to know your IT environment
  - Security Lifecycle Review (SLR)
- Provide Security awareness training for all personnel
- **Develop Information Security policies & Incident Response Plan**
- Implement perimeter security & internal segmentation
  - Install Next-Gen firewalls & use the Threat Intelligence Cloud
- Implement two-factor authentication
- Protect & manage Endpoints
  - Local Admin, Encrypt & Install Traps
- Implement Cloud security (Aperture)
- ……………

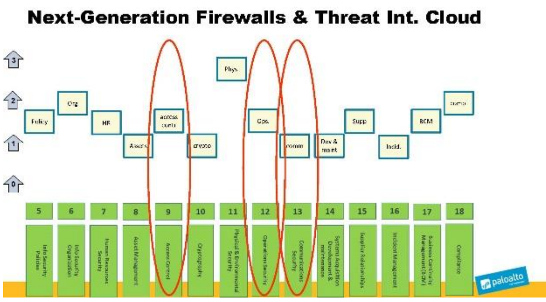


Your step-by-step security plan

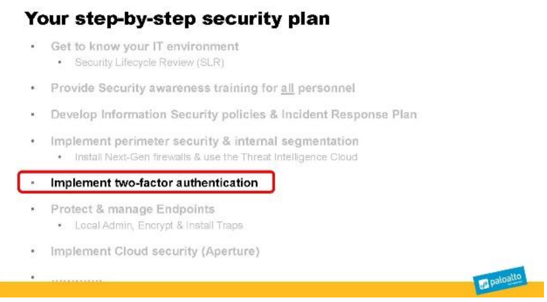
- Get to know your IT environment
  - Security Lifecycle Review (SLR)
- Provide Security awareness training for all personnel
- Develop Information Security policies & Incident Response Plan
- **Implement perimeter security & internal segmentation**
  - Install Next-Gen firewalls & use the Threat Intelligence Cloud
- Implement two-factor authentication
- Protect & manage Endpoints
  - Local Admin, Encrypt & Install Traps
- Implement Cloud security (Aperture)
- ……………



Perimeter security and segmentation

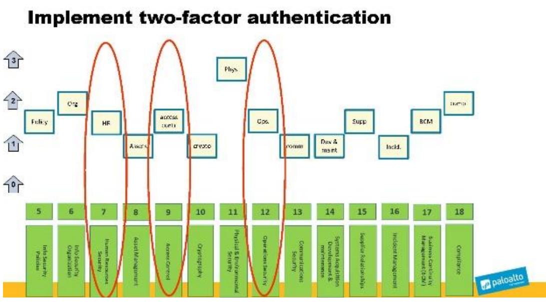


Next-Generation Firewalls & Threat Int. Cloud

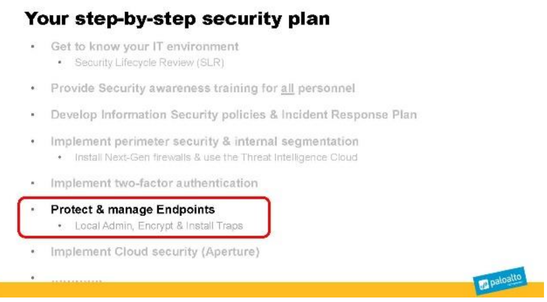


Your step-by-step security plan

- Get to know your IT environment
  - Security Lifecycle Review (SLR)
- Provide Security awareness training for all personnel
- Develop Information Security policies & Incident Response Plan
- Implement perimeter security & internal segmentation
  - Install Next-Gen firewalls & use the Threat Intelligence Cloud
- **Implement two-factor authentication**
- Protect & manage Endpoints
  - Local Admin, Encrypt & Install Traps
- Implement Cloud security (Aperture)
- ……………

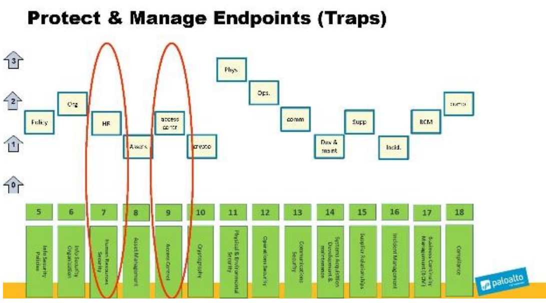


Implement two-factor authentication

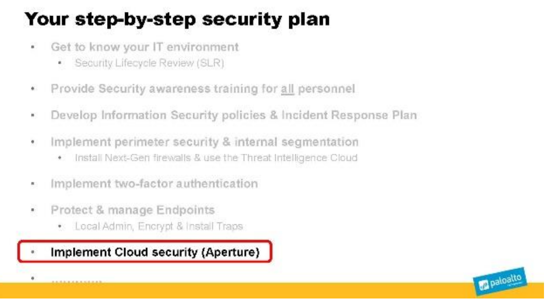


Your step-by-step security plan

- Get to know your IT environment
  - Security Lifecycle Review (SLR)
- Provide Security awareness training for all personnel
- Develop Information Security policies & Incident Response Plan
- Implement perimeter security & internal segmentation
  - Install Next-Gen firewalls & use the Threat Intelligence Cloud
- Implement two-factor authentication
- **Protect & manage Endpoints**
  - **Local Admin, Encrypt & Install Traps**
- Implement Cloud security (Aperture)
- ……………

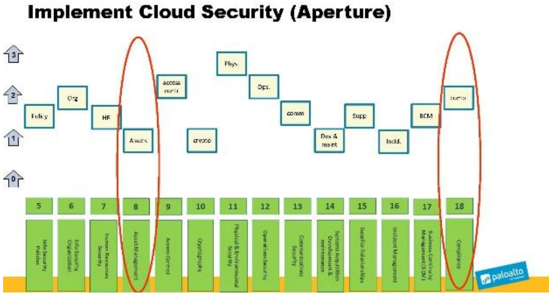


Protect & Manage Endpoints (Traps)



Your step-by-step security plan

- Get to know your IT environment
  - Security Lifecycle Review (SLR)
- Provide Security awareness training for all personnel
- Develop Information Security policies & Incident Response Plan
- Implement perimeter security & internal segmentation
  - Install Next-Gen firewalls & use the Threat Intelligence Cloud
- Implement two-factor authentication
- Protect & manage Endpoints
  - Local Admin, Encrypt & Install Traps
- **Implement Cloud security (Aperture)**
- ……………



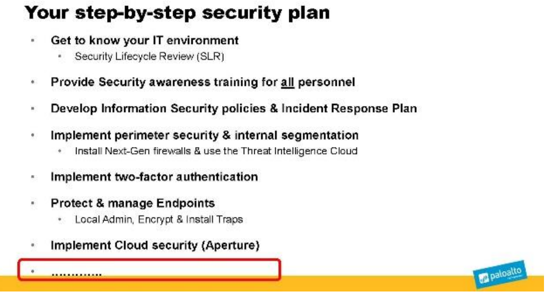
Implement Cloud Security (Aperture)

3
2
1
0

Policy
Org
HR
Assets
access contr.
crypto
Phys.
Ops.
comm
Dev & maint
Supp
Incid.
BCM
comp.

5	6	7	8	9	10	11	12	13	14	15	16	17	18
Info Security Policies	Info Security Organization	Human Resources Security	Asset Management	Access Control	Cryptography	Physical & Environmental Security	Operations Security	Communications Security	Systems Acquisition Development & maintenance	Supplier Relationships	Incident Management	Business Continuity Management (BCM)	Compliance

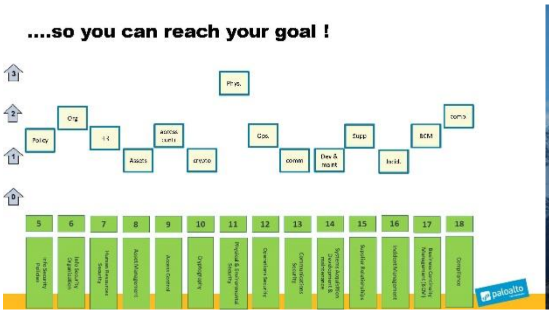
paloalto



Your step-by-step security plan

- Get to know your IT environment
  - Security Lifecycle Review (SLR)
- Provide Security awareness training for **all** personnel
- Develop Information Security policies & Incident Response Plan
- Implement perimeter security & internal segmentation
  - Install Next-Gen firewalls & use the Threat Intelligence Cloud
- Implement two-factor authentication
- Protect & manage Endpoints
  - Local Admin, Encrypt & Install Traps
- Implement Cloud security (Aperture)
- ………….

paloalto



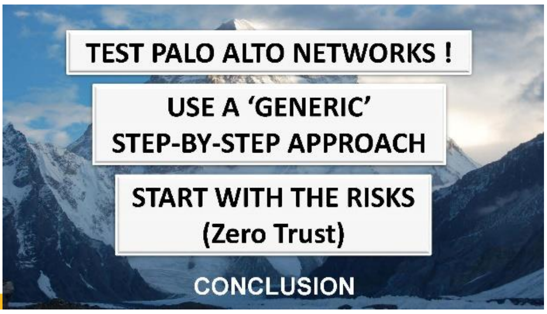
....so you can reach your goal !

3
2
1
0

Policy
Org
HR
access contr.
Assets
crypto
Phys.
Ops.
comm
Dev & maint
Supp
Incid.
BCM
comp.

5	6	7	8	9	10	11	12	13	14	15	16	17	18
Info Security Policies	Info Security Organization	Human Resources Security	Asset Management	Access Control	Cryptography	Physical & Environmental Security	Operations Security	Communications Security	Systems Acquisition Development & maintenance	Supplier Relationships	Incident Management	Business Continuity Management (BCM)	Compliance

paloalto



TEST PALO ALTO NETWORKS !

USE A 'GENERIC' STEP-BY-STEP APPROACH

START WITH THE RISKS (Zero Trust)

CONCLUSION

THANK YOU FOR YOUR ATTENTION !

FStreefland@PaloAltoNetworks.com
nl.linkedin.com/in/fredstreefland
+31 6 28461593

IBM Watson Health

PRIVACY & DATA PROTECTION SUMMIT

16-17 November 2017 | Radisson Blu Hotel | Berlin | Germany

Stewart Thompson
MA, BA (Mod) Comp. Sci
CDPP, MICS

Privacy Officer

IBM Watson Health

November 17th, 2017

IBM
© IBM 2017

IBM Watson Health IBM

- Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

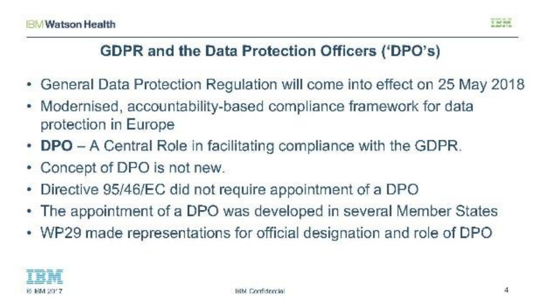
IBM
© IBM 2016 IBM Confidential 2

IBM Watson Health

The Data Protection Officer (DPO)

Who Needs one?
Who Should it be?
What should they do?
challenges and the future.

IBM
© IBM 2017



IBM Watson Health IBM

GDPR and the Data Protection Officers ('DPO's)

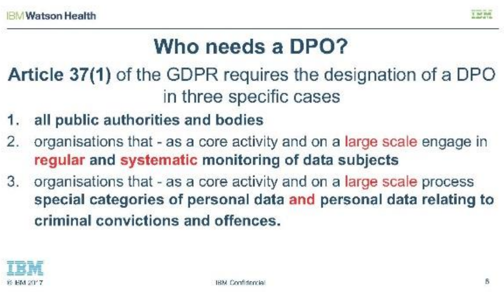
- General Data Protection Regulation will come into effect on 25 May 2018
- Modernised, accountability-based compliance framework for data protection in Europe
- **DPO** – A Central Role in facilitating compliance with the GDPR.
- Concept of DPO is not new.
- Directive 95/46/EC did not require appointment of a DPO
- The appointment of a DPO was developed in several Member States
- WP29 made representations for official designation and role of DPO

IBM
© IBM 2017 IBM Confidential 4

IBM Watson Health

Who needs a DPO?

© IBM 2017 IBM Confidential

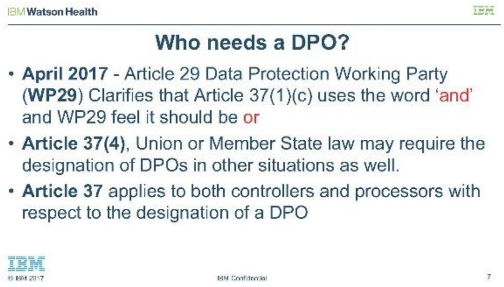

IBM Watson Health

Who needs a DPO?

Article 37(1) of the GDPR requires the designation of a DPO in three specific cases

1. **all public authorities and bodies**
2. organisations that - as a core activity and on a large scale engage in **regular and systematic monitoring of data subjects**
3. organisations that - as a core activity and on a large scale process **special categories of personal data and personal data relating to criminal convictions and offences.**

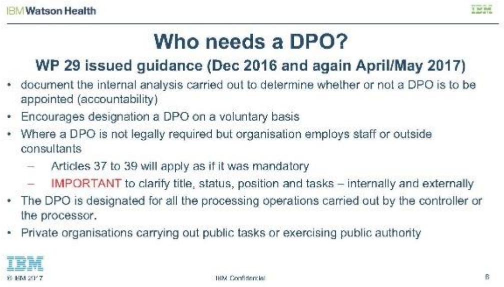
© IBM 2017 IBM Confidential 6


IBM Watson Health

Who needs a DPO?

- **April 2017** - Article 29 Data Protection Working Party (**WP29**) Clarifies that Article 37(1)(c) uses the word 'and' and WP29 feel it should be or
- **Article 37(4)**, Union or Member State law may require the designation of DPOs in other situations as well.
- **Article 37** applies to both controllers and processors with respect to the designation of a DPO

© IBM 2017 IBM Confidential 7

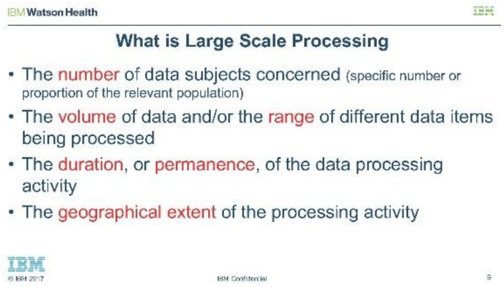

IBM Watson Health

Who needs a DPO?

WP 29 issued guidance (Dec 2016 and again April/May 2017)

- document the internal analysis carried out to determine whether or not a DPO is to be appointed (accountability)
- Encourages designation a DPO on a voluntary basis
- Where a DPO is not legally required but organisation employs staff or outside consultants
  - Articles 37 to 39 will apply as if it was mandatory
  - IMPORTANT to clarify title, status, position and tasks – internally and externally
- The DPO is designated for all the processing operations carried out by the controller or the processor.
- Private organisations carrying out public tasks or exercising public authority

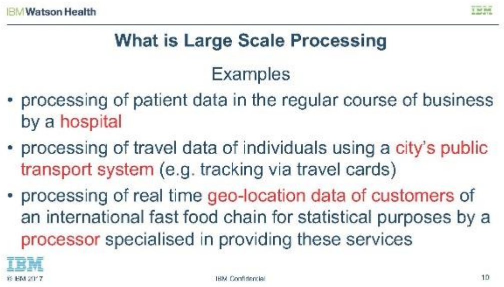
© IBM 2017 IBM Confidential 8


IBM Watson Health

What is Large Scale Processing

- The number of data subjects concerned (specific number or proportion of the relevant population)
- The volume of data and/or the range of different data items being processed
- The duration, or permanence, of the data processing activity
- The geographical extent of the processing activity

© IBM 2017 IBM Confidential 9

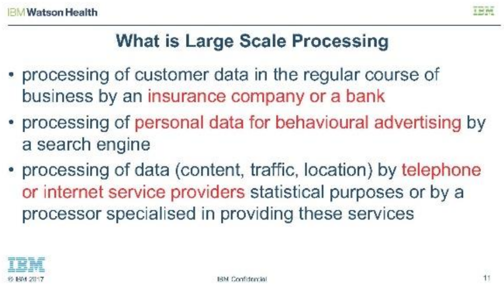

IBM Watson Health

What is Large Scale Processing

Examples

- processing of patient data in the regular course of business by a hospital
- processing of travel data of individuals using a city's public transport system (e.g. tracking via travel cards)
- processing of real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialised in providing these services

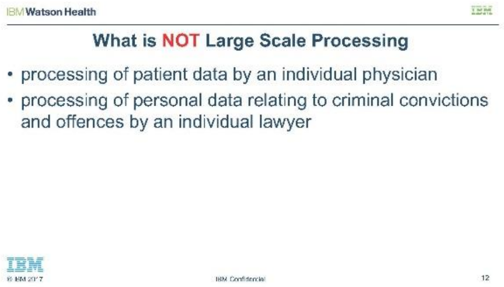
© IBM 2017 IBM Confidential 10


IBM Watson Health

What is Large Scale Processing

- processing of customer data in the regular course of business by an insurance company or a bank
- processing of personal data for behavioural advertising by a search engine
- processing of data (content, traffic, location) by telephone or internet service providers statistical purposes or by a processor specialised in providing these services

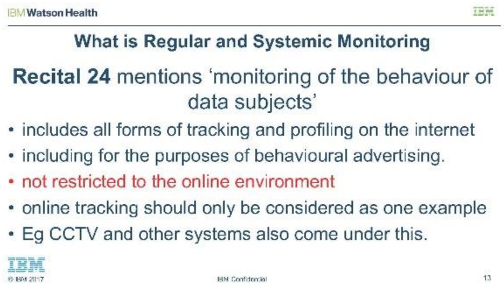
© IBM 2017 IBM Confidential 11


IBM Watson Health

What is NOT Large Scale Processing

- processing of patient data by an individual physician
- processing of personal data relating to criminal convictions and offences by an individual lawyer

© IBM 2017 IBM Confidential 12

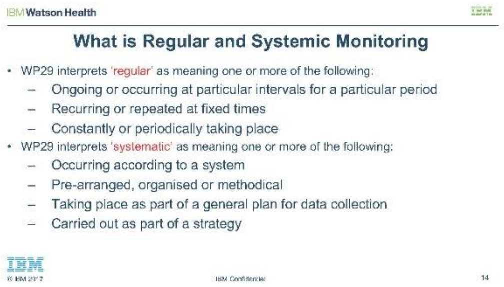

IBM Watson Health

What is Regular and Systemic Monitoring

Recital 24 mentions 'monitoring of the behaviour of data subjects'

- includes all forms of tracking and profiling on the internet
- including for the purposes of behavioural advertising.
- not restricted to the online environment
- online tracking should only be considered as one example
- Eg CCTV and other systems also come under this.

© IBM 2017 IBM Confidential 13


IBM Watson Health

What is Regular and Systemic Monitoring

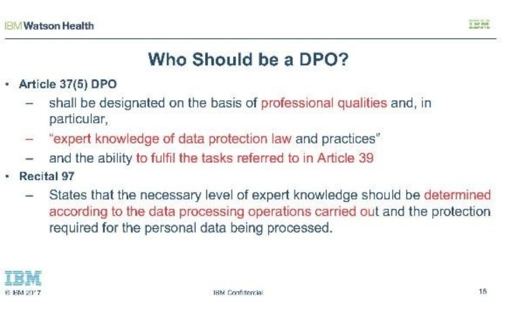
- WP29 interprets 'regular' as meaning one or more of the following:
  - Ongoing or occurring at particular intervals for a particular period
  - Recurring or repeated at fixed times
  - Constantly or periodically taking place
- WP29 interprets 'systematic' as meaning one or more of the following:
  - Occurring according to a system
  - Pre-arranged, organised or methodical
  - Taking place as part of a general plan for data collection
  - Carried out as part of a strategy

© IBM 2017 IBM Confidential 14

IBM Watson Health

Who should be a DPO?

© IBM 2017 IBM Confidential

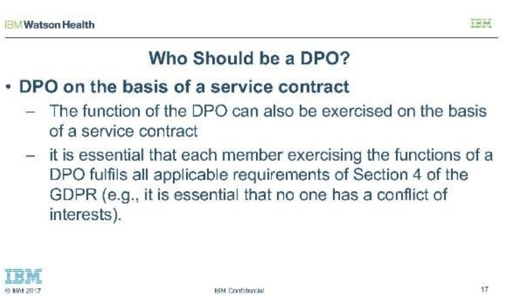


IBM Watson Health IBM

Who Should be a DPO?

- Article 37(5) DPO
  - shall be designated on the basis of professional qualities and, in particular,
  - "expert knowledge of data protection law and practices"
  - and the ability to fulfil the tasks referred to in Article 39
- Recital 97
  - States that the necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed.

IBM © IBM 2017 IBM Confidential 18



IBM Watson Health IBM

Who Should be a DPO?

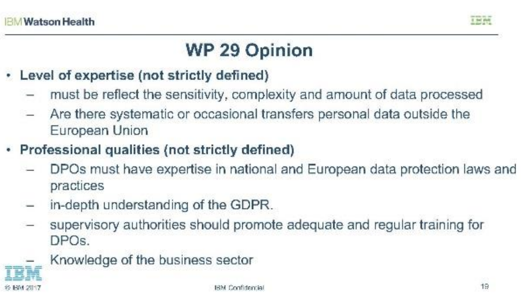
- **DPO on the basis of a service contract**
  - The function of the DPO can also be exercised on the basis of a service contract
  - it is essential that each member exercising the functions of a DPO fulfils all applicable requirements of Section 4 of the GDPR (e.g., it is essential that no one has a conflict of interests).

IBM © IBM 2017 IBM Confidential 17

IBM Watson Health

Lack of Clarity

© IBM 2017 IBM Confidential

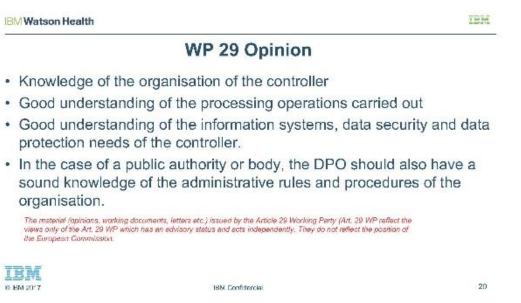


IBM Watson Health IBM

WP 29 Opinion

- **Level of expertise (not strictly defined)**
  - must be reflect the sensitivity, complexity and amount of data processed
  - Are there systematic or occasional transfers personal data outside the European Union
- **Professional qualities (not strictly defined)**
  - DPOs must have expertise in national and European data protection laws and practices
  - in-depth understanding of the GDPR.
  - supervisory authorities should promote adequate and regular training for DPOs.
  - Knowledge of the business sector

IBM © IBM 2017 IBM Confidential 19



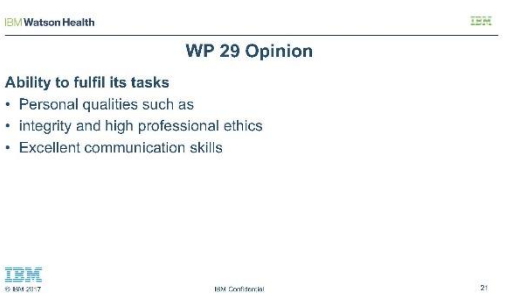
IBM Watson Health IBM

WP 29 Opinion

- Knowledge of the organisation of the controller
- Good understanding of the processing operations carried out
- Good understanding of the information systems, data security and data protection needs of the controller.
- In the case of a public authority or body, the DPO should also have a sound knowledge of the administrative rules and procedures of the organisation.

The material (opinions, working documents, letters etc.) issued by the Article 29 Working Party (Art. 29 WP reflect the views only of the Art. 29 WP which has an advisory status and acts independently. They do not reflect the position of the European Commission.

IBM © IBM 2017 IBM Confidential 20



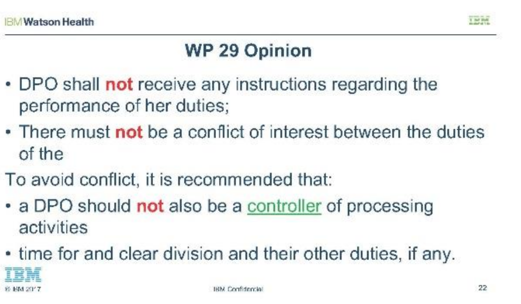
IBM Watson Health IBM

WP 29 Opinion

Ability to fulfil its tasks

- Personal qualities such as
- integrity and high professional ethics
- Excellent communication skills

IBM © IBM 2017 IBM Confidential 21



IBM Watson Health IBM

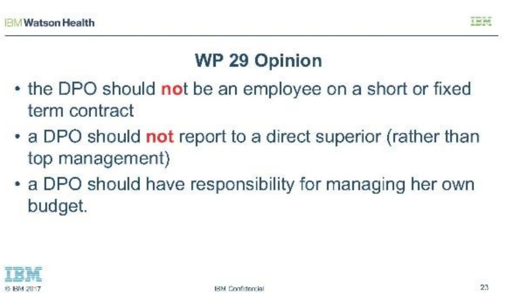
WP 29 Opinion

- DPO shall **not** receive any instructions regarding the performance of her duties;
- There must **not** be a conflict of interest between the duties of the

To avoid conflict, it is recommended that:

- a DPO should **not** also be a controller of processing activities
- time for and clear division and their other duties, if any.

IBM © IBM 2017 IBM Confidential 22

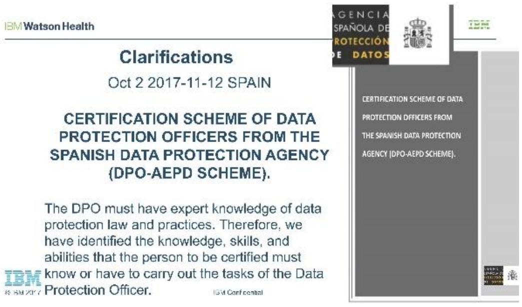


IBM Watson Health IBM

WP 29 Opinion

- the DPO should **no**t be an employee on a short or fixed term contract
- a DPO should **not** report to a direct superior (rather than top management)
- a DPO should have responsibility for managing her own budget.

IBM © IBM 2017 IBM Confidential 23



IBM Watson Health IBM

Clarifications

Oct 2 2017-11-12 SPAIN

CERTIFICATION SCHEME OF DATA PROTECTION OFFICERS FROM THE SPANISH DATA PROTECTION AGENCY (DPO-AEPD SCHEME).

The DPO must have expert knowledge of data protection law and practices. Therefore, we have identified the knowledge, skills, and abilities that the person to be certified must know or have to carry out the tasks of the Data Protection Officer.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

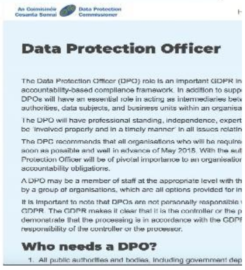
CERTIFICATION SCHEME OF DATA PROTECTION OFFICERS FROM THE SPANISH DATA PROTECTION AGENCY (DPO-AEPD SCHEME).

IBM © IBM 2017 IBM Confidential

Clarifications

November 3rd Ireland

Guidance issued on www.gdprandyou.ie that reflects WP29 guidance



An Coimisinéir Cosanta Sonraí Data Protection Commissioner

Data Protection Officer

The Data Protection Officer (DPO) role is an important GDPR in
accountability-based compliance framework. In addition to supp
DPOs will have an essential role in acting as intermediaries betv
authorities, data subjects, and business units within an organisa

The DPO will have professional standing, independence, expert
be 'involved properly and in a timely manner' in all issues relatin

The DPC recommends that all organisations who will be require
soon as possible and well in advance of May 2018. With the aut
Protection Officer will be of pivotal importance to an organisatior
accountability obligations.

A DPO may be a member of staff at the appropriate level with th
by a group of organisations, which are all options provided for in

It is important to note that DPOs are not personally responsible
GDPR. The GDPR makes it clear that it is the controller or the p
demonstrate that the processing is in accordance with the GDPF
responsibility of the controller or the processor.

Who needs a DPO?

1. All public authorities and bodies, including government dep

What should they do? – What is the role of a DPO?

- **Article 38(1)** DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.
- **Article 38(3)** DPO does not receive any instructions regarding the exercise of [his or her] tasks.
- **Article 35(2)** specifically requires that the controller shall seek advice of the DPO when carrying out a DPIA.
- **Article 39(1)(c),** tasks the DPO with the duty to provide advice where requested as regards the [DPIA] and monitor its performance pursuant to Article 35.

What should they do? – What is the role of a DPO?

- perform their duties and tasks in an independent manner. **Recital 97**
- tasks and duties do not result in a conflict of interests. **Article 38(6)**
- cooperate with the supervisory authority
- act as a contact point for the supervisory authority **Article 39(1)(d) and (e),**
- acts as a contact point for the performance of the tasks of the Supervisory Authority mentioned in **Article 57**
- Support the supervisory authority for the exercise of its investigative, corrective, authorisation, and advisory powers **Article 58**

What should they do? – What is the role of a DPO?

- **Article 39(2) Risk Based Approach** - requires that the DPO 'have due regard to the risk associated with the processing operations, taking into account the nature, scope, context and purposes of processing'.
- **Under Article 30(1) and (2), - Record Keeping** – responsibility of Controller and Processor – but in practical terms the DPO

What should they do? – What is the role of a DPO? WP29 states a DPO Shall

- collect information to identify processing activities
- analyse and check the compliance of processing activities
- inform, advise and issue recommendations to the controller /processor
- be invited to participate regularly in meetings with management.

What should they do? – What is the role of a DPO? WP29 states a DPO Shall

- Be present where decisions with data protection implications are taken.
- Have all information passed in a timely manner in order
- Have their opinion given due weight
- be promptly consulted once a data breach or another incident has occurred.

What should they do? – What is the role of a DPO? WP29 states a DPO Shall

- Ensure that controllers and data subjects are informed about their data protection rights, obligations and responsibilities and raise awareness about them;
- Give advice and recommendations about the interpretation or application of the data protection rules;
- Create a register of processing operations within the institution

What should they do? – What is the role of a DPO? WP29 states a DPO Shall

- notify the EDPS those that present specific risks (so-called prior checks);
- Ensure data protection compliance within her institution
- Handle queries or complaints on request by the institution, the controller, other person(s), or on her own initiative

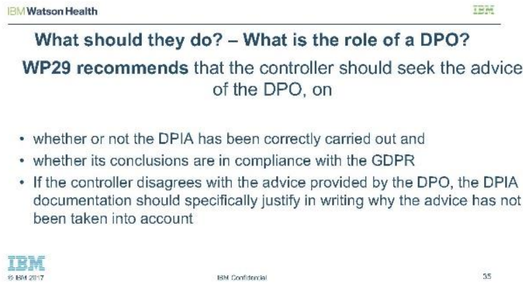
What should they do? – What is the role of a DPO?

- the controller or processor could develop guidelines that set out when the DPO must be consulted.
- In case of disagreement document the reasons for not following the DPO's advice.

What should they do? – What is the role of a DPO?

WP29 recommends that the controller should seek the advice of the DPO, on

- whether or not to carry out a data protection impact assessment (DPIA)
- what methodology to follow when carrying out a DPIA
- whether to carry out the DPIA in-house or whether to outsource it
- what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects



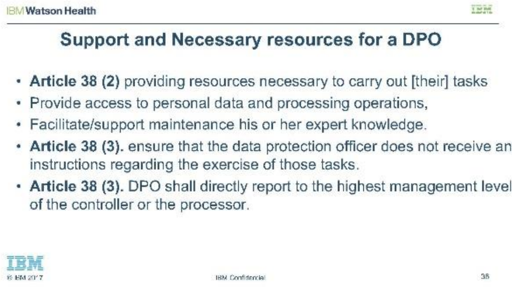
IBM Watson Health

What should they do? – What is the role of a DPO?

WP29 recommends that the controller should seek the advice of the DPO, on

- whether or not the DPIA has been correctly carried out and
- whether its conclusions are in compliance with the GDPR
- If the controller disagrees with the advice provided by the DPO, the DPIA documentation should specifically justify in writing why the advice has not been taken into account

© IBM 2017 IBM Confidential 35

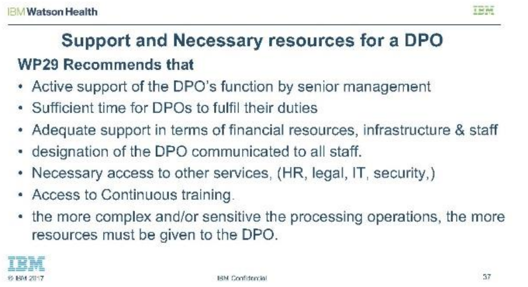


IBM Watson Health

Support and Necessary resources for a DPO

- **Article 38 (2)** providing resources necessary to carry out [their] tasks
- Provide access to personal data and processing operations,
- Facilitate/support maintenance his or her expert knowledge.
- **Article 38 (3).** ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks.
- **Article 38 (3).** DPO shall directly report to the highest management level of the controller or the processor.

© IBM 2017 IBM Confidential 36



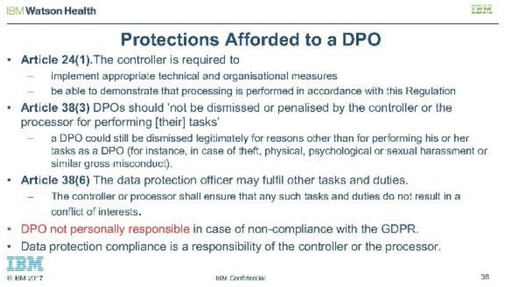
IBM Watson Health

Support and Necessary resources for a DPO

WP29 Recommends that

- Active support of the DPO's function by senior management
- Sufficient time for DPOs to fulfil their duties
- Adequate support in terms of financial resources, infrastructure & staff
- designation of the DPO communicated to all staff.
- Necessary access to other services, (HR, legal, IT, security,)
- Access to Continuous training.
- the more complex and/or sensitive the processing operations, the more resources must be given to the DPO.

© IBM 2017 IBM Confidential 37

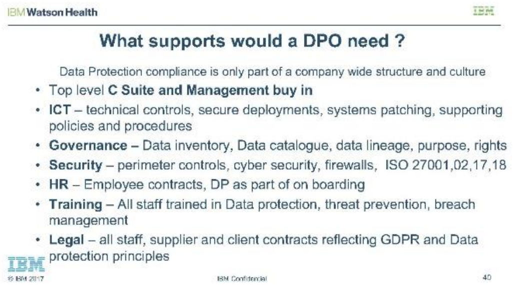


IBM Watson Health

Protections Afforded to a DPO

- **Article 24(1).**The controller is required to
  - implement appropriate technical and organisational measures
  - be able to demonstrate that processing is performed in accordance with this Regulation
- **Article 38(3)** DPOs should 'not be dismissed or penalised by the controller or the processor for performing [their] tasks'
  - a DPO could still be dismissed legitimately for reasons other than for performing his or her tasks as a DPO (for instance, in case of theft, physical, psychological or sexual harassment or similar gross misconduct).
- **Article 38(6)** The data protection officer may fulfil other tasks and duties.
  - The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.
- DPO not personally responsible in case of non-compliance with the GDPR.
- Data protection compliance is a responsibility of the controller or the processor.

© IBM 2017 IBM Confidential 38



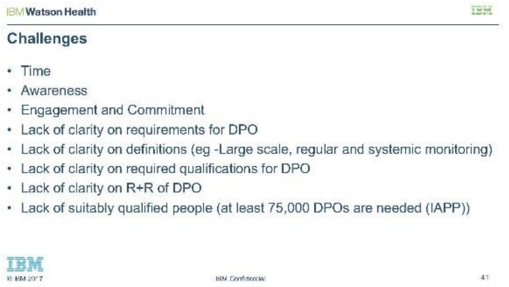
IBM Watson Health

What supports would a DPO need ?

Data Protection compliance is only part of a company wide structure and culture

- Top level **C Suite and Management buy in**
- **ICT** – technical controls, secure deployments, systems patching, supporting policies and procedures
- **Governance –** Data inventory, Data catalogue, data lineage, purpose, rights
- **Security** – perimeter controls, cyber security, firewalls, ISO 27001,02,17,18
- **HR** – Employee contracts, DP as part of on boarding
- **Training** – All staff trained in Data protection, threat prevention, breach management
- **Legal** – all staff, supplier and client contracts reflecting GDPR and Data protection principles

© IBM 2017 IBM Confidential 40

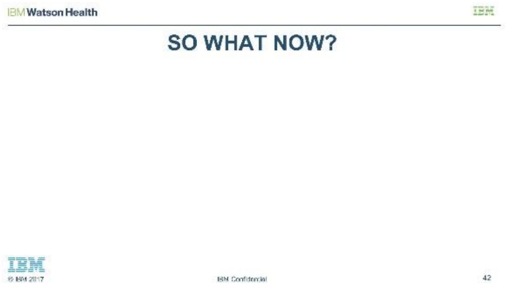


IBM Watson Health

Challenges

- Time
- Awareness
- Engagement and Commitment
- Lack of clarity on requirements for DPO
- Lack of clarity on definitions (eg -Large scale, regular and systemic monitoring)
- Lack of clarity on required qualifications for DPO
- Lack of clarity on R+R of DPO
- Lack of suitably qualified people (at least 75,000 DPOs are needed (IAPP))

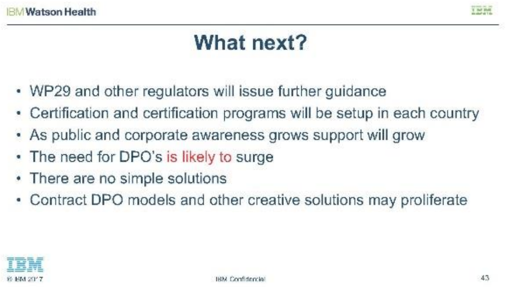
© IBM 2017 IBM Confidential 41



IBM Watson Health

SO WHAT NOW?

© IBM 2017 IBM Confidential 42

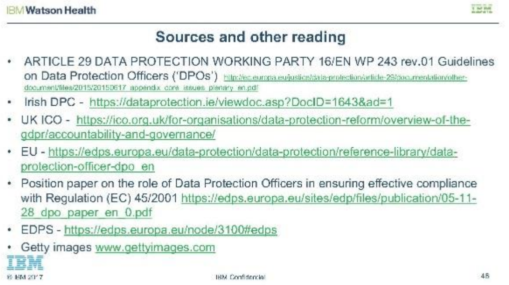


IBM Watson Health

What next?

- WP29 and other regulators will issue further guidance
- Certification and certification programs will be setup in each country
- As public and corporate awareness grows support will grow
- The need for DPO's is likely to surge
- There are no simple solutions
- Contract DPO models and other creative solutions may proliferate

© IBM 2017 IBM Confidential 43



IBM Watson Health

Sources and other reading

- ARTICLE 29 DATA PROTECTION WORKING PARTY 16/EN WP 243 rev.01 Guidelines on Data Protection Officers ('DPOs') http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf
- Irish DPC - https://dataprotection.ie/viewdoc.asp?DocID=1643&ad=1
- UK ICO - https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/accountability-and-governance/
- EU - https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en
- Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001 https://edps.europa.eu/sites/edp/files/publication/05-11-28_dpo_paper_en_0.pdf
- EDPS - https://edps.europa.eu/node/3100#edps
- Getty images www.gettyimages.com

© IBM 2017 IBM Confidential 45