GDPR for Technology & Cybersecurity Professionals - Training Overview

Session 1: Background, Objectives & Structure	
Subject: A Brief History of Privacy in the European Union *The concept of privacy has been around for millennia, but with the exception of a few philosophical treatises, was not truly formalised in Europe until the Universal Declaration of Human Rights was ratified on December 10th, 1948.* Session Objective: In order to provide the requisite context for the training program, it is necessary to briefly touch on what privacy actually is, and just as importantly, what it is *not*.	09:00 – 10:30
Subject: GDPR - Background *The **General Data Protection Regulation** (**GDPR**) (Regulation (EU) 2016/679) is a regulation (i.e. law) by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.* Session Objective: For appropriate context, we will discuss 1) where the GDPR came from, 2) what it hopes to correct from the previous Directive, and 3) what it is designed to achieve.	
Subject: GDPR - Principles & Rights *The GDPR, and privacy as it is seen in the EU, is predicated on 7 core Principles and 6 Data Subject Rights. The 173 Recitals and 99 Articles are simply the instructions on how these are to be implemented and maintained.* Session Objective: At a very high level, the GDPR is an instruction manual for the protection of personal data. An explanation of the actions to be taken by organisation will help keep these Principles and Rights at the forefront.	
Subject: GDPR - Lawful Basis for Processing *There are 6 accepted lawful bases for processing personal data. Every organisation must determine which of these apply, then implement appropriate and effective measures and be able to demonstrate compliance.* Session Objective: A brief overview of the 6 lawful bases for processing to enable business-level conversations.	
Morning Break	10:30 – 10:45

GDPR for Technology & Cybersecurity Professionals - Training Overview

Session 2: Major Information Technology Provisions	
Subject - Anonymisation vs. Pseudonymisation *The primary solution for reducing both the impact of GDPR compliance and reducing the inherent risk of processing personal data is to get rid of everything you don't need. While similar, anonymised and pseudonimised data result in very different levels of effort for compliance.* Session Objective: To understand the differences between these two concepts and the impact your choice will have.	10:45 – 12:15
Subject - Online Identifiers *The GDPR makes subtle, but specific references to online identifiers including IP addresses and cookies. This requirement ties the GDPR to the upcoming ePrivacy Regulation (2017/0003 (COD)) which will have significant impact on all forms of "electronic communications".* Session Objective: A brief introduction to the ePrivacy Regulation and its impact on GDPR preparations.	
Subject - Concept of Main Establishment *The location of equipment used to process personal data has less impact on GDPR readiness preparations than the location of the organisation's "main establishment", but this does not mean other locations can be ignored.* Session Objective: To understand the impact of location of technology / equipment on compliance efforts.	
Subject - Enforcement of Data Subject Rights *The technology implications related to the support of data subject rights has, by far, the most impact on technology. The exact requirements will depend on the applicable lawful basis for processing making the choice of the utmost importance.* Session Objective: To discuss real-world impact on technology related to the enforcement of data subject rights.	
Lunch Break	12:15 – 13:15

GDPR for Technology & Cybersecurity Professionals - Training Overview

Session 3: Major Information Security Provisions	
Subject - Network and Information Security as a Legitimate Interest *While not a 'get out of jail free card', personal data that can be demonstrated as being "strictly necessary and proportionate for the purposes of ensuring network and information security", can be processed under the umbrella of 'legitimate interest'.* Session Objective: While there should be few circumstances in which personal data is necessary to protect personal data, use of this option must be understood and justified.	13:15 – 14:45
Subject - Data Protection by Design and Default (DPbD²) *Data protection by design is not designated a Principle under GDPR, but it's close. Similar to how a Software Development Life Cycle (SDLC) ensures that security is built in to each stage of development, DPbD² must be implemented in all security processes to account for privacy.* Session Objective: To develop an appreciation for the intent of DPbD² and how to integrate some basic processes into existing security programs.	
Subject – "Appropriate Technical and Organisational Measures" *Like all regulations, the GDPR does not define what 'appropriate is. Nor should they. Instead, they are assuming a security program will contain all processes defined in industry accepted good practices. Unless an organisation can demonstrate that the entire security program meets the core tenets of confidentiality, integrity and availability (C.I.A.) they will never be able to demonstrate 'appropriate'.* Session Objective: To define what a supervisory authority would expect to see in a security program appropriate to the protection of personal data.	
Subject - Breach Notification *The notification of personal data breaches to the supervisory authority attracts significant text in both the Recitals (85, 86, 87 & 88) and Articles (33 & 34). Failure to meet the defined requirement also attracts significant penalties and repercussions.* Session Objective: To understand how the GDPR requirements go beyond just incident response and disaster recovery.	
Afternoon Break	14:45 – 15:00

GDPR for Technology & Cybersecurity Professionals - Training Overview

Session 4: Way Forward	
Subject - Data Discovery *From a technical perspective, the first step is to determine exactly what data you have and where it is. All of it. While this should already be in place, GDPR makes this step a crucial one. "We didn't know we had it." is not an argument the supervisory authorities will accept.* Session Objective: To understand the steps necessary to conduct an *appropriate* data discovery exercise.	15:00 – 16:30
Subject - Business Process Mapping *It is not enough to know what data you currently have, you have to know how additional data makes its way into your systems. It is only with a combination of data discovery and business process mapping that the business and legal sides can make a determination of lawful basis for processing.* Session Objective: To define the single most important task of the technology personnel in the implementation phase of the GDPR readiness project.	
Subject - Governance *For most organisations the implementation of GDPR is going to result in significant changes to both operational process and business culture. In order to create the necessary change, maintenance of GDPR must be governed by the highest levels of leadership.* Session Objective: To discuss the impact of Governance on GDPR compliance.	
Subject - Discussion, Q&A	