‘GDPR FOR SMES’ TRAINING COURSE

27th APRIL - DAY 1

9:00 - 10:30 1. Introduction

- The notions of ‘privacy’ and ‘personal data protection’ and their conceptualizations
- Privacy and personal data protection as fundamental rights; their functioning, distinction and rationale; and their relation to other rights
- General introduction to the personal data protection regulative framework (key European laws, guidelines and best practices)
- Introduction to the new EU regulatory framework for personal data protection (General Data Protection Regulation), pending reforms and their implications for EU/EEA Member States and Switzerland
- Conceptual changes in the new EU regulatory framework for personal data protection: principle of accountability, risk-based approach, new data subject rights, etc.

10:30 - 10:50 Coffee Break

10:50 - 12:20 2. Main principles of European personal data protection

- Definition of personal data
- Principles (lawfulness, accuracy, accountability, etc., incl. ‘new’ ones: data protection by default and data protection by design)
- Legal bases for processing data
- Data subject’s rights (access rights, incl. ‘new’ ones: data portability, right to be forgotten, etc.)
- Re-use of personal data
- Data anonymization and pseudonymization

Practical exercise:
-Exercising data subject’s rights: access, rectification, etc.

12:20 - 13:20 Lunch break

13:20 - 14:50 3. Controllers and processors:

- The data protection actors;
- Definitions of controllers and processors
- Role and relationship between the two
- The principle of accountability
- Controller and processor obligations
- The issue of consent: Conditions, exemptions, consent and vulnerable people (e.g. children)

Practical exercise:
- Consent form (indicative)
- Privacy policy (indicative)

14:50 - 15:10 **Coffee Break**

15:10 - 16:40 **4. The ePrivacy Regulatory framework**

- Analysis on current legal framework and recent law-making developments
- Soft law in the form of codes of conduct and other guidance
- The issue of the relationship between the ePrivacy regulatory framework and the GDPR
- Consent and basic data protection principles under the ePrivacy lens
- Confidentiality of communications
- Cookies & other tracking technologies
- Big data and data analytics in the ePrivacy context

16:40 - 17:00 **Coffee Break**

17:00 - 18:30 **5. Data Protection Officer (DPO)**

- When do you need a DPO?
- Functioning of a DPO (in-house & outsourced)
- Roles and activities of the DPO
- Competences of the DPO
- How to become a DPO?

Practical exercise:
-DPO certification

18:30 **One-to-one Questions and Answers**

20:00 **Dinner (Optional)**

28th APRIL - DAY 2

9:00 - 10:30 6. Supervision, liability and sanctions

- Data Protection Authorities (DPA)s
- European Data Protection Board (EDPB)
- One-stop-shop and consistency mechanism
- Remedies
- Liabilities and penalties

Practical exercise:
-Failures to comply and responsibilities

10:30 - 10:50 Coffee break

10:50 - 12:50 7. GDPR sector-specific compliance

- Defining legitimate ground
- Recruitment
- ICT usage at the workplace (including BYOD)
- ICT usage outside the workplace
- Workplace monitoring (i.e., relating to time and attendance, video monitoring systems, location)
- Specific employment context of a Member State
- Customer relationship management

Practical exercise:
-Processing of employee personal data when using company vehicles

12:20 - 13:20 Lunch Break

13:20 - 14:50 8. Issues related to sensitive data

- The evolving nature of health data
- The place for health data within the GDPR as special (sensitive) data
- Other forms of special data
- Extra requirements incumbent upon the processors of special data
- Obtaining consent for the use of health data
- Anonymisation issues and health data
- The need to implement organisational measures when dealing with special data
- The need to perform a Data Protection Impact Assessment with Sensitive Data

14:50 - 15:10 Coffee Break

15:10 - 16:40 9. International dimension of data protection

- Mechanisms for the transfer of personal data to the third countries (adequacy, binding corporate rules [BCR], standard contractual clauses [SCC], consent, etc.; transfers within an organisation)
- Extraterritorial application of GDPR
- Trans-Atlantic data protection (incl. a brief introduction to the US privacy law)
- Passenger Names Records (PNR)

16:40 - 17:00 Coffee Break

17:00 - 18:30 10. Data protection impact assessment (DPIA)

- The concepts of impact assessments and DPIAs
- Position of DPIA in the GDPR
- Occurrences when a DPIA must be conducted
- Steps of a DPIA based on art. 35 GDPR
- Risk to the right to the protection of personal data and its treatment

Practical exercise:
-Conducting a DPIA for mHealth applications