



EXCLUSIVE TSAARO ACADEMY NOTES GIVEAWAY



academy.tsaaro.com

About Tsaaro Academy

"It's not easy to build trust and manage risks at the same time"

Just getting a certification won't minimise nor guarantee your business from potential threats. It requires constant efforts and maintenance in securing the system from threats.

We at Tsaaro Academy provide the right training as per the international market standards to help data privacy professionals get access to the right skills to support their organisation with data privacy risks.

Our Official Partners



Featured in



1. Rationale for Data Protection

Early 1970s witnessed the advent of the increased use of computer to process individual's information. This led to the rising concerns regarding the adverse impact of processing on the privacy of individuals. The laws related to privacy, tort, secrecy and confidentiality were already in existence in the EU Member States but the automated storage of personal data and hike in cross border trade created a gap in the regulation to protect the privacy. The European Union regulators identified the need to balance the personal freedom and privacy, and the free flow of information to support international trade at very early stage.

2. Human Rights Law

2.1. Universal Declaration of Human Rights (UDHR)

UDHR was adopted on 10th December 1948 by the General Assembly of the United Nations to avoid the atrocities like World War II. This framework established universal values and traditions: 'the inherent dignity and the equal and inalienable rights of all members of the human race in the foundation of freedom, justice, and peace in the world'. It provided equal human rights to each individual living on earth.

This framework contains specific human rights for right to a private and family life and to freedom of expression.

Article 12- Right to private life and associated freedoms: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Article 19- Right to freedom of expression: Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Article 29 (2): In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.

Article 12 provide the right to private life and associated freedoms but Article 29 (2) shows that the rights are not absolute rather there are some limitations.

2.2. European Convention on Human Rights (ECHR)

On the lines of UDHR, in 1950, Council of Europe drafted European Convention on Human Rights and invited member states to sign it. This treaty was enforced on 3 September 1953 and it is only binding to member states of Council of Europe.

ECHR derives power from its enforcement mechanism. European Court of Human Rights examines the breaches of fundamental rights enshrined under ECHR and ensures that states comply with the obligations under the ECHR. Decisions of the Court are binding in the nature and can result in amendments in the member state laws.

Article 8: Right to Privacy, states that

(1) Everyone has the right to respect for his private and family life, his home and his correspondence.

(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

This provision resembles Article 12 of the UDHR and protects individual's right of personal information to remain private.

Article 10 (1): Right of freedom of expression

Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

These rights are also not absolute. A breach of Right to Privacy can be justified with public interest, but only if the personal data is used in necessary and proportional manner. Limitations of right to freedom of expression are set forth in Article 10(2)

The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or the rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

3. Early Laws and Regulations

Many European countries took a lead to regulate this area by incorporating data protection laws in national laws whereas three countries; Spain, Portugal and Austria, took a step further and added data protection as a fundamental right under their constitutions.

Some other instruments were framed for data protection by the international bodies including OECD and EU. In 1968, Council of Europe came up with Recommendation 509 on human rights and modern scientific and technological developments, following this in 1973 and 1974 Council of Europe framed two Resolutions 73/22 and 74/29, which established principles for the protection of personal data in automated databanks in the private and public sectors. Further, in 1980, Organisation for Economic Co-operation and Development (OECD) published Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ('Guidelines').

3.1. OECD Guidelines

OECD is an organisation that promotes policies to achieve sustainable economic growth and employment and increasing standard of living in OECD member states as well as non-member states. The Guidelines published on 23 September 1980 by the OECD, lays down basic rules to govern transborder data flows and protection of personal information and privacy. These guidelines are not legally binding. The guidelines were framed in close association with Council of Europe and hence,

shows similarities with the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

Interestingly, the Guidelines does not differentiate between public and private sectors and also it is technology neutral and does not make any distinction between personal information collected through automated, non-automated (electronic) means or otherwise. The principles introduced by the Guidelines include, collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability. The principles also support the free flow of information between OECD member countries.

3.2. Convention 108

The first legally binding international instrument was compiled by the Council of Europe in the form of The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108'). Council of Europe invited its member and non-member to sign it on 28 January 1981. This Convention requires signatories to take required steps towards adopting its principles in domestic legislations. As suggested in the title, it particularly focuses on automated processing of personal data.

3.3. Convention 108+

After 30 years of Convention 108's enforcement, Convention 108 Advisory Committee laid down foundation for a modernisation protocol on 11 January 2011. It particularly addresses the challenges imposed by the use of new information and communication technologies like Internet of Things (IoTs), artificial intelligence and machine learning.

In May 2018, the final version of a 'Protocol amending the Convention of the Protection of Individuals with regard to Automated Processing of Personal Data' was approved and signed by 21 states. This amended Convention 108 is referred as Convention 108+. Many of its principles, procedures and enforcement mechanisms are similar to that of GDPR. Recital 105 of the GDPR, directs the European Commission to take into consideration the accession of Convention 108 by a third country, while considering the adequacy status of such third country under the GDPR

4. The need for a harmonised European Approach

OECD Guidelines and Convention 108, both aimed to introduce a harmonised approach for their respective member states but could not achieve it reason being the implementation of the principles was left to the discretion of the member states. This discretion exercised by the member states led to the development of a diversified data protection regimes.

5. Data Protection Directive

To unify these diversified data protection regimes, European Commission asked European Parliament to prepare a proposal for a directive harmonising data protection laws in 1976. Soon European parliament tabled Proposal for a Council Directive Concerning the Protection of Individual in Relation to the Processing of Personal Data which raised concerns regarding the impediment in the cross border flow of data due to lack of uniform safeguards in relation to the right to privacy.

After considering the proposal, European Commission came up with Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('Data Protection Directive', or 'Directive'). Directive is a type of legislation in the European Union which is binding in nature but it leaves the implementation (choice of form and methods) to the national authorities.

The Directive incorporated the principles of Convention 108. The aim of the Directive was to provide protection to the individual's fundamental privacy rights with free flow of the data from one member state to another, while adhering with Article 8 and 10 of the ECHR. Unfortunately, the aim could not fulfil because of significant differences in the way member states have implemented the Directive. Report of European Commission in 2003, confirmed that the varied practices are becoming hurdles for the business to take full advantage of the internal market.

6. Charter of Fundamental Rights

6. Charter of Fundamental Rights

On 7 December 2000, the Charter of Fundamental Rights was signed by the presidents of the European Parliament, the Council and the Commission. This Charter stems out of the EU Treaty, CJEU case law, ECHR, and EU member states' constitutional traditions. This charter was awarded more authority by making it legally binding by the Treaty of Lisbon in 2009.

Article 8 of the Charter:

- 1) Everyone has the right to the protection of personal data concerning him or her;
- (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
- (3) Compliance with these rules shall be subject to control by an independent authority.

This Article particularly protects the personal data of the individuals. It reflects the core values of data protection i.e. fair processing, purpose specific processing, legitimate basis, establishment of supervisory authority to oversee compliance and it also provides right to access and rectification. Any limitation to these rights must be in accordance with Article 52 of the Charter.

7. Treaty of Lisbon

Treaty of Lisbon ("Lisbon Treaty") was signed by the EU member states on 13 December 2007 and came into effect on 1 December 2009. It amended the Treaty on European Union and the Treaty Establishing the European Community (renamed the 'Treaty on the Functioning of the European Union', or 'TFEU'). It also protects the personal data of the individuals.

Article 16 of the Treaty of Lisbon:

(1) that everyone has the right to the protection of personal data concerning him or her.

(2) the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States where carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

This provision binds all EU institutions to protect individuals when processing personal data.

8. General Data Protection Regulation

To overcome the lack of harmonisation of the Directive, the Commission launched a review of the Directive in 2009. Following this in 2012, the Commission proposed General Data Protection Regulation (“GDPR” or “Regulation”). Regulation is a EU legislation which is fully binding and apply directly to the member states. For its application member states need not to transpose the Regulation’s laws in the domestic legislation. For GDPR, a trilogue was started between the European Commission, the European Parliament and the Council of the EU. In May 2016, all parties agreed and the Regulation was published in the Official Journal of the European Union and was enforced on 25 May 2018.

The Regulation is uniformly applicable on all member states but at the same time it allows the members to make further specific rules in some situations. Such as:

- Where there are already sector-specific laws in place (for example, in relation to the employee data)
- Archiving purposes in the public interest, scientific or historical research purposes, statistical purposes

- Processing of 'special categories of personal data'
- Processing in compliance with a 'legal obligation'

Major changes made in the Regulation as compare to Directive:

- Stronger rights of individuals
- Data protection by design and by default
- Concept of "Accountability"
- Increase in the powers of supervisory authorities
- Territorial scope

9. Related Legislations

9.1. The Law Enforcement Data Protection Directive

Along with GDPR, the European Commission also proposed a directive for the 'protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data' ('Law Enforcement Data Protection Directive', or LEDP Directive). It came into force on 5 May 2016. Since it is a Directive, a period of two years (until 6 May 2018) was given to the member states to transpose it in national laws. The aim of this legislation is to harmonise the rules for processing of personal data by the law enforcement agencies of the member states.

9.2. The ePrivacy Directive

In addition to GDPR, there are specific laws, ePrivacy Directive, to regulate the processing of personal data by the public communications networks. The GDPR clarifies that it will not impose additional obligations on the public communications networks. It also talks about amending the ePrivacy directive to ensure the consistency between both. The EU is planning to push ePrivacy Regulation.

Post Brexit

After exit from EU, UK is no more regulated by the EU GDPR rather they have developed an independent data protection law, Data Protection Act, 2018 (DPA) which was amended after the Brexit and now it is collectively termed as UK GDPR. Now, for EU it is considered as a third country.

The personal data transfer from EU to UK relies on adequacy status which was announced on 28 th June 2021. This adequacy status is with a sunset clause, which means the adequacy status will be reassessed in four years from its announcement.





KICK START YOUR CAREER

**Enquire For Training at
Tsaaro Academy**

**info.academy@tsaaro.com
+91 93353 36454**