1. Rationale for data protection

During the early 1970s there was an increase in the use of computers to process information about individuals. This coincided with the development of the European Economic Community, which resulted in a rise in trans-border trade, and therefore more sharing of personal information, facilitated by the development of computer technology.

Rapid progress in the field of electronic data processing and the first appearance of mainframe computers allowed public administrations and large enterprises to set up extensive data banks and to improve the collection, processing and sharing of personal information. Added to this was the fact that computers, in combination with the development of telecommunications, were opening up new opportunities for data processing on an international scale.

Although these developments offered considerable advantages in terms of efficiency and productivity, they also gave rise to concerns that these otherwise positive advancements would have an adverse impact on the privacy of individuals and that this would be exacerbated when personal information was transferred across international boundaries.

Within the individual state legal systems in Europe there were already some rules aimed at protecting the personal information of individuals, such as laws on privacy, tort, secrecy and confidentiality. However, it was recognised that the automated storage of personal information and the rise in cross-border trade called for new standards that allowed individuals to exercise control over their personal information, while allowing the free international flow of information necessary to support international trade.

The challenge was to frame these standards in a way that maintains a balance between concerns at a national level for personal freedom and privacy and the ability to support free trade at the European Economic Community level.
2. Human rights law

International human rights law is built on agreements between countries to promote and protect human rights at the international, regional and domestic level.

2.1 Universal Declaration of Human Rights

The obvious starting point as a basis for framing standards for the protection of individuals was the Universal Declaration on Human Rights (also called the Human Rights Declaration), adopted on 10 December 1948 by the General Assembly of the United Nations. The Human Rights Declaration recognised what have now become universal values and traditions acknowledging ‘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’.

The Human Rights Declaration contains specific provisions in connection with the right to a private and family life and to freedom of expression regardless of frontiers. The principles enshrined in the Human Rights Declaration have in fact provided the basis for all subsequent European data protection laws and standards.

The right to a private life and associated freedoms is contained in Article 12 of the Human Rights Declaration, which states:

\[
\text{No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.} \\
\]

Another fundamental aspect in the Human Rights Declaration is the right to freedom of expression as set out in Article 19:

\[
\text{Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.} \\
\]

The provisions in Article 19 may seem at first to be at odds with the provisions of Article 12, particularly where the exercise of Article 19 might result in the invasion of privacy contrary to Article 12. This apparent conflict is, however, reconciled in Article 29(2), which states that individual rights are not absolute and that there will be instances where a balance must be struck to limit their exercise:

\[
\text{In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.} \\
\]
2.2 European Convention on Human Rights

In Rome, in 1950, the Council of Europe invited individual states to sign the European Convention on Human Rights (ECHR), an international treaty to protect human rights and fundamental freedoms. Based on the Human Rights Declaration, it entered into force on 3 September 1953. The ECHR applies only to member states and therefore is referred to as a ‘closed instrument’. All Council of Europe member states are a party to the ECHR, and new members are expected to ratify the ECHR at the earliest opportunity. Parties to the ECHR undertake to provide these rights and freedoms to everyone within their jurisdiction.

The ECHR is a powerful instrument because of the scope of the fundamental rights and freedoms it protects. These include the right to life, prohibition of torture, prohibition of slavery and forced labour, right to liberty and security, right to a fair trial, no punishment without law, respect for private and family life, freedom of thought, conscience and religion, freedom of expression, freedom of assembly and association, right to marry, right to an effective remedy and prohibition of discrimination.\(^2\)

The ECHR is also significant because there is a system of enforcement established in Strasbourg in the form of the European Court of Human Rights, which examines alleged breaches of the ECHR and ensures that states comply with their obligations under the ECHR. Rulings of the European Court of Human Rights are binding on the states concerned and can lead to an amendment of legislation or a change in practice by national governments. At the request of the Committee of Ministers of the Council of Europe, the Court of Human Rights may also give advisory opinions concerning the interpretation of the ECHR and the protocols.

On 1 November 1998 the court system was restructured into a single full-time Court of Human Rights.\(^3\)

Article 8 of the ECHR echoes Article 12 of the Human Rights Declaration and provides that:

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

\(\text{(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.}\)\(^4\)

This article therefore protects the rights of individuals for their personal information to remain private, but again, this is not an absolute right and necessity and proportionality may justify the breaching an individual’s privacy rights in the public interest.
Whilst Article 8 deals with the right to privacy, Article 10 protects the right of freedom of expression and the right to share information and ideas across national boundaries. Article 10(1) of the ECHR reads:

*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.*

This right is also qualified so as to protect the privacy of individuals, as 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.*

Both the Human Rights Declaration and the ECHR inherently recognise a need for balance between the rights of individuals and the justifiable interference with these rights, which is a recurring theme within data protection law.

### 3. Early laws and regulations

From the late 1960s to the 1980s a number of countries, mostly in Europe, took the lead in implementing legislation aimed at controlling the use of personal information by government agencies and large companies. These included Austria, Denmark, France, Federal Republic of Germany, Luxembourg, Norway and Sweden, with legislation planned in several others. In three European countries, Spain, Portugal and Austria, data protection was also incorporated as a fundamental right in the Constitution.\(^5\)

In light of this trend, the Council of Europe decided to establish a framework of specific principles and standards to prevent unfair collection and processing of personal information. This was the result of concern that, in the context of emerging technology, national legislation did not adequately protect the ‘right to respect for his private and family life, his home and his correspondence’ under Article 8 of the ECHR. This concern led in 1968 to the publication of Recommendation 509 on Human Rights and Modern and Scientific Technological Developments.

In 1973 and 1974 the Council of Europe built on this initial work with Resolutions 73/22 and 74/29, which established principles for the protection of personal data in automated databanks in the private and public sectors, respectively, the objective being to set in motion the development of national legislation based on these resolutions. This was re-
garded as an urgent requirement due to the concern that there was already a divergence between the laws of the member states in this area. It was becoming increasingly apparent that comprehensive protection of personal information would be effective only through further reinforcement of such national rules by means of binding international standards.

Other significant initiatives in the early 1980s came from the Organisation for Economic Co-operation and Development (OECD) and the Council of Europe in the form of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.

3.1 OECD Guidelines

Broadly speaking, the role of the OECD is to promote policies designed to achieve the highest sustainable economic growth and employment and a rising standard of living, in both OECD member countries and nonmember countries, while maintaining financial stability and thus contributing to the development of the world economy. OECD membership extends beyond Europe and includes a number of major jurisdictions.

In 1980, OECD developed Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (‘Guidelines’) laying out basic rules governing trans-border data flows and the protection of personal information and privacy in order to facilitate the harmonisation of data protection law between countries. (See the box outlining the principles in the Guidelines.)

The Guidelines were prepared in close cooperation with the Council of Europe and the European Community and were published on 23 September 1980. They are not legally binding but are intended to be flexible and to serve either as a basis for legislation in countries that have no data protection legislation, or as a set of principles that may be built into existing legislation.

Because OECD membership extends beyond Europe, the Guidelines have a far-reaching effect. The emphasis is on cooperation with other countries so that gaps will not arise in the implementation of the Guidelines among the OECD member states. The OECD reaffirmed its commitment to the Guidelines in declarations made in 1985 and 1998.

In developing the Guidelines, the OECD made every effort to ensure consistency with the principles being developed on behalf of the Council of Europe, which means there are distinct similarities between the Guidelines and the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.

The aim of the Guidelines is to strike a balance between protecting the privacy and the rights and freedoms of individuals without creating any barriers to trade and allowing the uninterrupted flow of personal data across national frontiers.

The Guidelines do not draw any distinction between the public and private sectors. Importantly, they are neutral with regard to the particular technology used in that they do not make any distinction between automated and nonautomated
**OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**

The Guidelines introduce a set of principles that should be followed by data controllers processing personal information:

- **Collection Limitation Principle:** Personal information must be collected fairly and lawfully and with the knowledge or consent of the individual concerned.

- **Data Quality Principle:** Personal information must be relevant, complete, accurate and up to date.

- **Purpose Specification Principle:** The purpose for which the personal information is to be used must be specified at the time of collection, and any use must be compatible with that purpose.

- **Use Limitation Principle:** Any disclosure of personal information must be consistent with the purposes specified unless the individual has given consent or the data controller has lawful authority to do so.

- **Security Safeguards Principle:** Reasonable security safeguards must be taken against risks such as loss or unauthorised access, destruction, use, modification or disclosure of personal information.

- **Openness Principle:** There should be a general policy of openness with respect to the uses of personal information as well as the identity and location of the data controller.

- **Individual Participation Principle:** This sets out what an individual is entitled to receive from a data controller pursuant to a request for his or her personal information. This has become one of the most important aspects of subsequent data protection legislation.

- **Accountability Principle:** A data controller should be accountable for complying with measures that ensure the principles stated above.

The principles included in the Guidelines in connection with trans-border data flows are within the spirit of the aims of the OECD to advance the free flow of information between member countries and to avoid creating unjustified obstacles to the development of economic relations among member countries. The Guidelines state that:

- Member states should take into consideration the implications for other member countries of domestic processing and reexport of personal data.

- Member states should take all reasonable and appropriate steps to ensure that trans-border flows of personal data, including transit through a member country, are uninterrupted and secure.

- Member states should not restrict trans-border flows of personal data between themselves except where a country does not yet substantially observe the Guidelines, or where the reexport of personal data would circumvent its domestic privacy legislation.
systems, and that concentrating exclusively on computers might lead to inconsistency as well as opportunities for data controllers to circumvent national laws that implement the Guidelines by using nonautomatic means to process personal information. The emphasis of their work was to safeguard personal information, the processing of which might ‘pose a danger to privacy and individual liberties’.

3.2 Convention 108

The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) was adopted by the Council of Europe and opened for signature to the member states of the Council of Europe on 28 January 1981. The fact that it was not referred to as the European Convention was to signify that it was open for signature to countries outside Europe.

Convention 108 consolidates and reaffirms the content of the 1973 and 1974 resolutions and was the first legally binding international instrument in the area of data protection. It differs from the Guidelines in that it requires signatories to take the necessary steps in their domestic legislation to apply the principles it lays down in order to ensure respect for the fundamental human rights of all individuals with regard to processing of personal information.

In Convention 108 the Council of Europe took the view that those holding and using personal information in computerised form have a social responsibility to safeguard such personal information, particularly as, increasingly, decisions affecting individuals are based on information stored in computerised data files.

The preamble to Convention 108 states that its aim is to achieve greater unity between its members and to extend the safeguards for everyone’s rights and fundamental freedoms—in particular, the right to respect for privacy, taking into account the increasing transfer across frontiers of personal data undergoing automatic processing.

Convention 108 is the first binding international instrument to set standards for the protection of individuals’ personal data whilst also seeking to balance those safeguards against the need to maintain the free flow of personal data for the purposes of international trade.
Convention 108 consists of three main parts:

- substantive law provisions in the form of basic principles (Chapter II);
- special rules on trans-border data flows (Chapter III); and
- mechanisms for mutual assistance and consultation between the parties (Chapter IV).  

3.2.1 Chapter II—Substantive law provisions

The principles in Chapter II are based on those contained in the 1973 and 1974 Council of Europe resolutions and are similar in many ways to those contained in the Guidelines:

- Personal information undergoing automatic processing shall be:
  - obtained and processed fairly and lawfully;
  - stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
  - adequate, relevant and not excessive in relation to the purposes for which they are stored;
  - accurate and, where necessary, kept up to date; and
  - preserved in a form that permits identification of the individuals for no longer than is required for the purpose for which the information is stored.

- Appropriate security measures must be taken for the protection of personal information stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

- Personal information revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life or criminal convictions (referred to as 'special categories of data'), may not be processed automatically unless domestic law provides appropriate safeguards.

- Individuals must have the right of communication, rectification and erasure of the personal information held.

When implementing Convention 108, signatories can include an exception to the provisions only when this is a 'necessary measure in a democratic society' (e.g., state security or criminal investigation) reflecting the proportionality requirements embodied in Articles 6, 8, 10 and 11 of the ECHR.
3.2.2 Chapter III — Trans-border data flows

Chapter III of Convention 108 also imposes some restrictions on trans-border flows of personal data to countries where the law does not provide protection.

Article 12 of Convention 108 provides that where transfers of personal information are made between signatories to Convention 108, those countries shall not impose any prohibitions or require any special authorisations for the purpose of the protection of privacy before such transfers can take place. The reason is that such states, by virtue of the fact that they are signatories to Convention 108, have agreed to the data protection provisions referred to in Chapter II and, as a result, they offer a certain minimum level of protection to the personal information transferred.

Derogation from the provisions is permitted only where the exporting country has in place specific rules in its national law for certain categories of personal data and the importing country does not provide equivalent protection or where the transfer is to a country that is not a party to Convention 108.

These provisions were further developed in the Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder data flows (‘Additional Protocol’), which opened for signature in 2001. The Additional Protocol was designed to address the fact that Convention 108 did not provide any measures for transfers of personal information to countries that were not signatories to Convention 108. The solution to this was the introduction of the concept of an ‘adequate’ (rather than an equivalent) level of protection for personal information transferred to states falling outside the jurisdiction of the exporting party, subject to exceptions where the transfer is made in the legitimate interests of the individual, is in the public interest or where the transfer is based on contractual clauses approved by the supervisory authority.\(^{10}\)

3.2.3 Chapter IV — Mutual assistance and consultation

Parties to Convention 108 must designate a supervisory authority to oversee compliance with data protection law and to liaise with supervisory authorities in other jurisdictions for purposes of consultation and mutual assistance regarding implementation. Supervisory authorities are also required to lend assistance to individuals in the exercise of their rights. These requirements were reinforced further by provisions in the Additional Protocol.

Convention 108 remains the only binding international legal instrument with a worldwide scope of application in the field of data protection that is open to any country, including countries that are not members of the Council of Europe.

4. The need for a harmonised European approach

European privacy law is built on the concept of international agreement on principles, with implementation left to the discretion of the member states. From the earliest days, it
was understood that member state discretion would require special effort to harmonise privacy regulation in an information society where the physical borders between the member states are less and less relevant.

4.1 Data Protection Directive

Despite the fact that the objective of Convention 108 and the Guidelines was to introduce a harmonised approach to data protection, a diverse set of data protection regimes was developing even amongst the small number of countries that adopted national laws based on them.

Convention 108 leaves open a variety of options for the implementation of the standards it contains, and it was perceived that the lack of a cohesive approach within the member states in adopting these principles could have serious implications for the fundamental rights of individuals as well as impede the concept of free trade enshrined in the Treaty of Rome.

The European Commission had been called upon by the European Parliament as early as 1976 to prepare a proposal for a directive harmonising data protection laws. Growing concerns regarding the diversity of national approaches to data protection legislation within member states was the catalyst for the Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data.¹¹

This proposal described the concerns of the European Commission with regard to the fragmented approach emerging and contained a framework directive for data protection. In this proposal the European Commission commented: ‘The diversity of national approaches and the lack of a system of protection at Community level are an obstacle to completion of the internal market. If the fundamental rights of data subjects, in particular their right to privacy, are not safeguarded at Community level, the cross-border flow of data might be impeded’.

The principles contained in Convention 108 were used as a benchmark by the European Commission in drawing up the framework directive because they constituted a common set of standards for those countries that had ratified Convention 108. The framework directive supplemented these general principles to provide a high level of equivalent protection, and to achieve this, the proposals were wide in their scope, extending the protections to both automated and nonautomated personal data and covering both public and private sectors.

The culmination of the work undertaken by the European Commission was 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 (also known as the Data Protection Directive, or simply the Directive). As the title suggests, the aim of the Directive is to further reconcile the protection of the fundamental rights of individuals with the free flow of data from one member state to another, maintaining consistency with Articles 8 and 10 of the ECHR.

Unfortunately, there are still significant differences in the ways member states have implemented and applied the Directive, making it difficult for businesses to take full advan-
tage of the benefits of the internal market. This was confirmed in the first report of the European Commission on the Directive, published in 2004.\textsuperscript{12}

In some cases the differences result from incorrect implementation of the Directive, which means that the law of the member state requires rectification. If the member state fails to remedy the position, the European Commission can issue infraction proceedings against it. In other cases, the differences may result from a member state’s implementation of the Directive that is within the margin of manoeuvre allowed, but which still may give rise to inconsistencies.

One example of the latter is in connection with the Directive’s prohibition on transferring personal information to countries outside the European Union without adequate protection. The national laws in the individual member states can vary significantly, which results in a complex process for multinational organisations trying to achieve compliance in a number of member states. Another example concerns the requirement for businesses to notify the data protection authorities of the details of their processing. The national laws of the member states can differ considerably as to their requirements in this regard, which can result in substantial bureaucracy and cost for businesses, particularly where the businesses are also transferring personal information to countries outside the EU.

The main focus of the European Commission has been on improving implementation in the member states and on a more consistent application and interpretation of the Directive. However, the divergence of national measures and practices implementing the Directive and the impact on this for businesses and individuals, together with the developments in technology since the Directive was drafted, has led the European Commission to initiate a comprehensive review. This is examined further in Chapter 3.

4.2 Charter of Fundamental Rights

The presidents of the European Parliament, the Council and the Commission signed and proclaimed the Charter of Fundamental Rights on behalf of their institutions on 7 December 2000 in Nice. Stemming from the EU Treaty, European Court of Justice case law, the European Union member states constitutional traditions and the European Convention on Human Rights, it further consolidates fundamental rights applicable within the EU.

The Charter includes the general principles set out in the ECHR but specifically refers to the protection of personal data. In December 2009, when the Treaty of Lisbon came into force, the Charter was given binding legal effect.

Articles 7 and 10 of the Charter reflect the provisions of the ECHR in Articles 8 and 10, respectively, and Article 8 deals specifically with data protection as follows:

\begin{itemize}
  \item[(1)] Everyone has the right to the protection of personal data concerning him or her;
  \item[(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; and
\end{itemize}
(3) Compliance with these rules shall be subject to control by an independent authority.\textsuperscript{13}

Article 8 therefore enshrines certain core values for the protection of personal data:

- The processing must be fair.
- The processing must be carried out for specified purposes.
- There must be legitimate basis for the processing.
- Individuals must have the right to access and rectification of personal data.
- There must be a supervisory authority to oversee compliance.

Any limitation to these rights must be in accordance with Article 52 of the Charter, which mirrors the limitations based on necessity and proportionality contained in the ECHR.

5. The Treaty of Lisbon

On 13 December 2007, the Treaty of Lisbon (Lisbon Treaty) was signed; it became effective on 1 December 2009.\textsuperscript{14} Its main aim is to strengthen and improve the core structures of the European Union to enable it to function more efficiently.

The Lisbon Treaty amends the EU’s two core treaties, the Treaty on European Union and the Treaty Establishing the European Community (renamed the Treaty on the Functioning of the European Union, or TFEU). Article 16(2) of TFEU provides that:

\begin{quote}
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 when 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.
\end{quote}

This provision ensures that all institutions of the European Union must protect individuals when processing personal data. There is a European Data Protection Supervisor whose role is to regulate compliance with data protection law within the institutions of the European Union, but the reference to ‘authorities’ implies that the national data protection authorities may also have jurisdiction in such matters.

Promoting a number of core values, including human dignity, freedom, democracy, equality, the rule of law and the respect for human rights, is one of the main objectives of the Lisbon Treaty. These values are common to all member states, and any European country wishing to become a member of the European Union must respect them. This is a significant development, because the treaty establishing the European Union did not mention fundamental rights at all.
The Lisbon Treaty describes the area of justice, freedom and security as being a high priority, and a significant change in this area is the introduction of one common legal framework for all EU activities, comprising one system through which the EU can govern.

This chapter has looked at the historical context and origins of European data protection law, including an overview of the key parts of the regulatory framework; Chapter 3 (‘Legislative Framework’) builds on this background by providing a more-detailed analysis of the key laws and regulations in place.

Evolution of Data Protection Law in Europe

1948 General Assembly of the United Nations creates The Universal Declaration of Human Rights recognising universal values and traditions—‘the inherent dignity and the equal and inalienable rights of all members of the human race’ to freedom, justice, and peace in the world.

1950 In Rome, the Council of Europe invites individual states to sign on to The European Convention on Human Rights (ECHR) to protect human rights and fundamental freedoms. Entered into force in 1953, it only applies to member states, who are expected to provide these rights and freedoms to everyone within their jurisdiction. It includes the European Court of Human Rights in Strasbourg to enforce the ECHR throughout the member states.

1951 The Treaty Establishing the European Coal and Steel Community (Treaty of Paris) set up regional institutions for governing coal and steel. Parties to the Treaty were France, West Germany, Italy, Belgium, Luxembourg, and the Netherlands.

1957 Treaty Establishing the European Economic Community (Treaty of Rome)

1965 Treaty Establishing a Single Council and a Single Commission of the European Communities (Merger Treaty) established the Common Market and created the European Commission, the Council of Ministers, the European Court of Justice, and the European Parliament.

1970 The German State of Hesse introduces the first modern privacy law.

1973 Sweden creates the Data Act, the first national privacy law.

1973–1974 Resolutions 73/22 and 74/29, are passed establishing principles for the protection of personal data in automated data banks in the private and public sectors respectively to set in motion the development of national legislation based on these resolutions.
1979 General data protection laws had been enacted in seven member states (Austria, Denmark, France, Federal Republic of Germany, Luxembourg, Norway and Sweden) with legislation planned in several others. In three European countries, Spain, Portugal, and Austria, data protection was also incorporated as a fundamental right in the Constitution.

1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) consolidates and re-affirms the 1973 and 1974 resolutions and is the first legally binding international instrument in the area of data protection. It differs from the OECD Guidelines in that it requires signatories to Convention 108 to take the necessary steps in their domestic legislation to apply the principles it lays down.

1986 The Single European Act amended the prior treaties and created an ‘internal market’ (effective 1992) and led to a single currency and an end to border regulation.


1995 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 (the Data Protection Directive or the Directive) further reconciled the protection of the fundamental rights of individuals with the free flow of data from one member state to another.


2000 Charter of Fundamental Rights of the European Union further consolidated fundamental rights applicable within the EU, and included the general principles set out in the ECHR but specifically refers to the protection of personal data.

2001 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows was designed to address the fact that Convention 108 did not provide for transfers of personal information to countries which are not signatories to Convention 108. It introduced the concept of an ‘adequate’ (rather than an equivalent) level of protection for personal information transferred to non-EU states.
ORIGINS AND HISTORICAL CONTEXT OF DATA PROTECTION LAW

2002 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (The e-Privacy Directive) deals with the regulation of a number of important issues such as confidentiality of information, treatment of traffic data, spam, and cookies.

2006 Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

2007 Treaty of Lisbon was designed to strengthen and improve the core structures of the European Union to enable it to function more efficiently. It made the 2000 Charter binding law. The Treaty established the European Data Protection Supervisor.