UNIO - *EU Law Journal*. Vol. 5, No. 2, July 2019, pp 92-102.

School of Law – University of Minho

The protection of personal data in the field of judicial cooperation in criminal matters: special reference to Directive (EU) 2016/680 of the European Parliament and of the Council

Maria Belén Sánchez Domingo*

ABSTRACT: The new European framework for the protection of personal data on freedom, security and justice is embodied, among other instruments, in EU Directive 2016/680 on the protection of natural persons with regards to the processing of personal data by competent authorities for criminal law purposes. This Directive protects fundamental rights, such as the right to the protection of personal data, as well as ensuring a high level of public security by facilitating the exchange of personal data between competent authorities within the Union, with the establishment of a legal system on the transfer of personal data.

KEYWORDS: fundamental rights – protection of personal data – processing of personal data – transfer of data – supervisory authority.

* Professor of Criminal Law at Rey Juan Carlos University, Madrid.

I. Introduction[1]

The adoption of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016[2], on the protection of natural persons with regards 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,[3] has led to the establishment of a specific framework for the protection and processing of personal data in the framework of criminal investigations and prosecutions. The Directive, along with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016,[4] on the protection persons with regards to the processing of personal data and on the free movement of such data, the main legislative instruments in the field of data protection,[5] aim at protecting natural persons with regards to the processing of personal data,[6] although the scope of the two instruments is different. Thus, the Regulation shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filling system or are intended to be included in a filing system (Article 1), but it shall never apply to the processing of personal data intended for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.[7] This is the reason why the Regulation will not be under consideration in this paper as our focus is on the analysis on the processing of personal data by competent authorities, in the framework of criminal investigations or criminal proceedings in accordance with the provisions of Directive 2016/680 itself.

Today, cross-border crime is one of the phenomena that requires a firm response from all States. Challenges which have arisen at both international and European

[1] This text is an updated version of the publication "*La transferencia de datos personales a terceros países y organizaciones internacionales según la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016*", published in Spain in the collective work *Los avances del espacio de Libertad, Seguridad y Justicia de la UE en 2017, coordinated by M.A. Gutiérrez Zarza, II Anuario ReDPE, La Ley.*

[2] *OJ L* 119/89, 4 May 2016.

[3] Directive replacing Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters: *OJ L* 350/60, 30 December 2008.

[4] *OJ L* 119/1, 4 May 2016 and replacing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on natural persons with regard to the processing of personal data and on the free movement of such data.

[5] However, other instruments should be mentioned which also aim to guarantee the protection of personal data, such as Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks; Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on consumer protection cooperation.

[6] Article 1 of Directive 2016/680 and Article 1 of Regulation 2016/679 respectively.

[7] Recital (19) of the Regulation: "*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, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should therefore not apply to processing activities intended for such purposes*".

level in the fight against this phenomenon, require EU Member States to adopt legal mechanisms that ensure effective action to deal with certain criminal activities such as terrorism. For this reason, the European Union has adopted measures aimed at coordinating all the Member States in the eradication and prevention of this phenomenon. These measures are a step toward effective action in the coordination, prevention and eradication of terrorism. It is worth highlighting the efforts that the European Union has been making to reinforce cross-border cooperation between the competent authorities in investigative and prevention functions. Those efforts aim at combating this form of criminality together with the establishment of policies directed at protection and prevention to counteract public security threats within the Union[8].

At the same time, the development of new information and communication technologies and, above all, the development of data transmission networks, basically the Internet, contribute to the realization of certain criminal behaviors which may affect the content of certain rights recognized for individuals, such as the protection of personal data, behaviors which require a response from the States themselves at both European and international level. Let us remember that the protection of personal data is a fundamental right as recognized in Article 8 of the Charter of Fundamental Rights of the European Union ("CFREU"), which states that *"Everyone has the right to the protection of personal data concerning him or her",* consolidating it as an autonomous fundamental right and not as a dimension of the right to privacy, also referred to in Article 7 of the CFREU[9]. In turn, Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) similarly enshrines the right to respect for private and family life. The Directive itself, in its Article 1, proclaims the protection of natural persons with regards to the processing of personal data as a fundamental right in accordance with the CFREU itself, as well as in Article 16, paragraph 1, of the Treaty on the Functioning of the European Union (TFEU),[10] which recognizes the right of everyone to the protection of personal data. At the same time, it should be noted that the CFREU, in the aforementioned Article 8, states that the respect and fulfillment of the obligations of protection shall be subject to control by an independent authority.

In this context, in order to strengthen prevention in the fight against terrorism, the Union provided, *inter alia*, the development of common rules on the protection of personal data. Thus, in the well-known multiannual programmes, such as the Hague Programme (2005-2009),[11] its priorities include effectively combating terrorism and

[8] In the Communication from the Commission to the European Parliament, the Council and the European Council, delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union: COM 2016 at the end of 2 April 2016 states that "*The European Agenda on Security has already proposed measures to address the main challenges for effective and sustainable action at EU level to fight terrorism and organized crime, specifically through better exchange of information between Member States' law enforcement authorities and with EU agencies, and by improving the interoperability of relevant databases and information systems*".

[9] Article 7: Respect for private and family life: Everyone has the right to respect for his or her private life, home and communications.

[10] Article 16.1: "*1. Everyone has the right to the protection of personal data concerning then. 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 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*".

[11] "Communication from the Commission to the Council and the European Parliament of 10 May

its causes. It contained proposals aimed at strengthening cooperation between the law enforcement authorities of the Member States, by improving the exchange of information between the various law enforcement and judicial authorities, as well as the objective of developing a European data protection framework. This objective was also reaffirmed in the Stockholm Programme (2010-2014),[12] which already established the basic informing principles regarding the processing of personal data. At the same time, the European Agenda on Security (2015-2019),[13] reiterates the need to achieve effective action in the framework of judicial cooperation, insists on the need to formulate measures that serve to address the main challenges facing the Union in the fight against terrorism and other forms of organized crime.[14]

The attacks on several European cities – such as Brussels, Nice, London – forced the European Union to adopt legislative measures with the aim of achieving effective action in the exchange of information between the various competent national and international authorities,[15] opting for confidence-building measures between law enforcement and judicial authorities of the different Member States, while guaranteeing a high level of public security by ensuring the exchange of personal data between competent authorities within the Union.

Precisely, the Directive marks the achievement of a certain degree of harmonization for the protection and free movement of personal data processed for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.[16] As is well known, the principle of mutual recognition of judicial decisions and sentences, the cornerstone of judicial cooperation in criminal matters, which has been operating as an alternative to any harmonization of criminal legislation by serving as a guiding criterion with regard to Community policy on freedom, security and justice, provided for in Article 82(1) of the TFEU, which imposes the combination of the principle of mutual recognition and approximation of criminal laws by stating that *"judicial cooperation in criminal matters within the Union shall be based on the principle of mutual recognition of judgments and judicial decisions and shall include the approximation of the laws and regulations of the Member States"*. With regards

2005 The Hague Programme: Ten priorities for the next five years. The Partnership for European renewal in the field of Freedom, Security and Justice": COM (2005) 184 final. *OJ C* 236, 24.9.2005.

[12] Stockholm Programme: An open and secure Europe serving and protecting citizens, OJ of the EU No. C 115/1, 4 May 2010: *"The Union must therefore respond to the challenge posed by the increasing exchange of citizens' personal data and the need to ensure the protection of privacy. The Union must secure a comprehensive strategy to protect citizens' data within the EU and in its relations with other countries. In those circumstances, it should promote the application of the principles set out in relevant Union instruments on data protection and the 1981 Council of Europe Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data as well as promoting accession to that Convention".*

[13] Communication from the Commission to the European Parliament, the Council and the European Council, delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union: COM 2016, 20 April 2016.

[14] Council Document 143491 EUCO79/14 of 14 June 2014, 'Presidency Conclusions, p. 2, paragraph 4, under the heading "Freedom, security and justice", which states that "in further developing the area of freedom, security and justice over the next years, it will be crucial to ensure the protection and promotion of fundamental rights, including data protection, while addressing security concerns, also in relations with third countries, and to adopt a strong EU General Data Protection framework by 2015".

[15] Recital (7) of the Directive: "*Ensuring a consistent and high level of protection of the personal data of natural persons and facilitating the exchange of personal data between competent authorities of Members States is crucial in order to ensure effective judicial cooperation in criminal matters and police cooperation*".

[16] Recital (15) loaf the Directive: providing for harmonized rules for the protection and the free movement of personal data.

to harmonization, this approach will help to increase trust between judicial authorities of different Member States of the Union,[17] as stated in Article 67(3) TFEU itself, the Union shall endeavor to *"ensure a high level of security through measures to prevent and combat crime, racism and xenophobia, and through measures for coordination and cooperation between police and judicial authorities and other competent authorities, as well as through the mutual recognition of judgments in criminal matters and, if necessary, through approximation of criminal laws"*.

II. Directive (EU) 2016/680 of the European Parliament and of the Council: general provisions, scope and definitions

The Directive, as set out in its own wording and in Recital (6), replaces Council Framework Decision 2008/977/JH of 27 of November 2008 ("FD"),[18] both of which share common features, although they differ in some other respects. The two instruments have the same structure; although the Directive is articulated in an extensive number of Articles (sixty-five) the Recitals being equally broader (one hundred and seven). At the same time, it should be stressed that the Directive in question follows the same tone as Council of Europe Convention 108,[19] the result of the important activity carried out by the Council of Europe regarding the protection of personal data.

With regards to the Convention, it should be pointed out that it is an internationally legally binding text in the field of data protection, and that has had an important influence on the other instruments drawn up within the European Union, by imposing the guidelines of a common model for personal data protection.[20] Its purpose is to ensure minimum standards of protection for every individual *vis-a-vis* the automatic processing of personal data, as stated in Article 1: *"...respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to the automatic processing of personal data relating to him ("data protection")*.

In turn, the Convention aims at harmonizing the laws of the Member States on the protection of personal data, inviting all non-Member States of the Council of Europe to accede to it. The Convention continues to form part of European legislation on the protection of personal data, as determined by the Directive itself in Recital (68).[21]

The Directive itself serves this purpose, in line with Recital (2), by preventing crime and by cooperation between judicial and police authorities on the protection of personal data. Thus, the Directive, on the one hand, protects the fundamental rights and freedoms of natural persons, in particular, the right to protection of personal data. On the other hand, it seeks to ensure a high level of public security by facilitating the exchange of personal data between competent authorities for the purposes of the

[17] Recital (15) of the Directive: *"The approximation of Member States' laws should not result in any lessening of the personal data protection they afford but should, on the contrary, seek to ensure a high level of protection within"*.
[18] Framework Decision implementing specifically in the fields of police and judicial cooperation in criminal matters, thus limited to the processing of personal data transmitted or made available between the Member States (Article 1 of the Framework Decision and reaffirmed in Recital 7).
[19] Of 28 January 1981, signed by Spain on 28 January 1982 and ratified on 27 January 1984, BOE (Spanish Official Journal) of 15 November 1985.
[20] Arenas Ramiro, *El Derecho Fundamental a la protección de datos personales en Europa* (Valencia, Tirant Lo Blanch, 2006), 153-157; Bru Cuadrado, E., "La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad", *Revista de Internet, Derecho y Política*, No. 5 (September, 2007): 82-83, https://idp.uoc.edu/.
[21] Establishing that the accession of the country to the Council of Europe Convention of 28 January 1981 is to be taken into account in relation to the international commitments entered into by third country or international organisation with regard to the transfer of data.

prevention, investigation and prosecution of crime, as well as for the enforcement of criminal penalties. It is an instrument that promotes trust between the police and judicial authorities of different Member States of the Union, in the exchange of information between the various authorities of the Member States with regards to the protection of personal data, while ensuring legal and public security.

Article 1 defines the aim and sets out the objectives of the Directive. It starts by establishing minimum standards for the protection of natural persons in the processing of personal data by competent authorities for the purposes of prevention, investigation and criminal proceedings.[22]

As in Recital (14), Article 2 provides that its scope is limited to the processing of personal data by competent authorities for the purposes of prevention, investigation or prosecution of criminal offences and also applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. Furthermore, the Directive shall not apply to the processing of personal data in the context of an activity which falls outside the scope of Union law and to the processing of personal data by Union institutions, bodies, offices or agencies.[23]

Regarding the specific content of the Directive, it shows certain similarities with Directive 95/46/EC, although in some respects a more exhaustive development can be observed. First, although it lists a series of definitions which coincide with those of Directive 95/46/EC and Convention 108, it introduces some novelties, such as the specific provision for what is meant by *"competent authority"*.

Thus, Article 3 tightens up definitions of *"personal data"*, *"processing"*, *"file system"*, *"competent authority"*, *"controller"*, *"processor"*, *"personal data breach"*, *"recipients"*. It also defines different categories of data classified as sensitive which require a series of minimum guarantees for their processing, such as *"genetic data"*, *"biometric data"*, and *"data concerning health"*. Although these definitions did not appear either in Convention 108 or in the Framework Decision 2008/977/JAI, nevertheless, both instruments referred to the same by classifying them as *"sensitive data"*, establishing a specific regime in relation to their processing. One new feature of this Directive is the definition of the concept of *"competent authority"*: "*any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security*." (Article 3, 7, a). It extends the concept of competent authority to those bodies or entities entrusted by Member State law to exercise public authority and public powers for the purpose of prevention, investigation or prosecution of criminal offences. Recital (12) of the Directive specifically refers to the police and law enforcement bodies as competent authorities for carrying out the activities concerning criminal investigations and prosecutions, which can also be extended to judges and prosecutors in the exercise of their judicial functions.

In turn, the Directive details the principles relating to the processing of personal data for the purposes of the investigation, prevention or detection of criminal offences in Articles 4 et seq., principles which coincide with those specified in Convention 108,

[22] It is reaffirmed in turn in Recital (11): "*The laying down of specific rules relating to 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*".

[23] As stated in Recital (11). Regulation (EC) No. 45/2001 of the European Parliament and of the Council, but adapted to Regulation (EU) 2016/679 (Recital 19), should apply in these cases.

Directive 95/46/EC and Framework Decision 2008/977/JHA, albeit with a more precise wording than that presented by the abovementioned normative texts. The Directive thus states that Member States shall provide for personal data to be processed lawfully, fairly and transparent in relation to the persons concerned and shall only be carried out for the specific purposes laid down by law. In Recital (26), it is specified that personal data shall be adequate and relevant in relation to the purposes for which they are processed, that is, for prevention, investigation and prosecution of criminal offences or sanctions, which requires a guarantee that the personal data collected shall not be excessive or kept for longer than strictly necessary for the purposes for which they are processed. Furthermore, it stresses that personal data may only be processed if the purpose of the processing cannot be obtained by other means. The specific purposes for which the processing of personal data is intended, for prevention, investigation or prosecution purposes, should be explicit and legitimate (Recital 29), with the obligation to be agreed at the time of collection of the personal data subject to processing.

Finally, with regard to the principle of accuracy[24] of personal data, the Directive imposes an obligation on the competent authorities, given the nature and purpose of the processing of personal data, that data which are inaccurate, incomplete or no longer up to date may not be transmitted or made available (Recital 32). Also, authorities should add necessary information in all transmissions of personal data. In addition, there is also an obligation to keep the data stored in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed (Article 4, 1, e).

III. Transfers of personal data to third countries or international organisations

As explained earlier, in accordance with Article 1, the establishment of rules concerning natural persons in the processing of personal data by competent authorities, in the prevention and investigation of criminal offences in order to ensure the exchange of data, Chapter V of the Directive, Articles 35-40, under the heading "*General principles for transfers of personal data"*, delimit the scope and requirements for authorizing transfers of personal data. Thus, these precepts allow the possibility of exchange of personal data by competent authorities to third countries or international organizations, for which it is necessary to comply with the following requirements:

- The transfer shall be necessary for the purposes set out in Article 1, that is, exclusively for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.
- In turn, transfers of personal data should be carried out only by "competent public authorities" acting as controllers, although the Directive itself, in Recital (64), requires an exception in the specific case where processors have received explicit instructions to carry out the transfer on behalf of controllers.

With regard to "competent authorities", referred to by the Article 3, a) and b),[25] it can be said that they are judges, prosecutors and even members of the State

[24] "R*ecital (30), a requirement which should not appertain to the accuracy of a statement, but as specified in the Directive, merely to the fact that a specific statement has been made*".

[25] Where "competent authority" is specified as follows: "*any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection*

Security Forces in the exercise of functions attributed to them as public authority. This is probably one of the most problematic points of the Directive, specifically in case members of the State's Security Forces decide to apply a repressive measure to a demonstration posing a threat to public security. Such action is related to the prevention or investigation of criminal offences. As is well known, this activity is conferred on the police, since it is the responsibility of the State Security forces and Corps to maintain public order. The Directive itself states that, coercive measures to repress a demonstration or a riot shall be considered as police activities focused on the detention or prevention of threats to public security (Recital 12). Therefore, in accordance with the literal interpretation of Article 3 of the Directive and the tasks assigned to a competent authority, it shall be able to carry out the free movement of personal data between law-enforcement authorities for judicial investigations.

When personal data are transferred or originated from another Member State, that Member State must give its prior authorisation for the transfer, in accordance with national law. However, such prior authorization shall not be required in cases where the transfer of personal data is necessary in order to prevent an immediate or serious threat to the public security of a Member State or, a third country or, to the essential interests of a Member State, provided that prior authorization cannot be obtained in good time (Article 35.2).

As for the fact that it must be considered an "immediate" and "serious" threat, the Directive says nothing about it, which can create interpretative issues in the delimitation of such concepts. However, Recital (65) specifies that the nature of the threat to the public security of a Member State shall be so immediate *"as to render it impossible to obtain prior authorisation in time",* without defining the criteria to be taken into account in relation to this requirement.[26]

In turn, so that the transfer of data may be performed, the third country or international organisation should ensure an "adequate level of protection",[27] which has to be decided by the Commission, thus providing legal certainty and uniformity, in which case no specific authorisation is required. The Directive itself, in Recital (67) as in Article 36, specifies the elements necessary for the Commission to assess the level of protection as adequate. Thus, on this point, it determines which Directive the Commission should take into account, whether that third country respects the rule of law, access to justice, international human rights norms and standards, as well as its general and sectoral law, criminal law and public policy.[28]

---

or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".

[26] This in turn is reiterated in Recital (12) of the Directive.

[27] See Judgment of the EU Court of Justice of 6 October 2015, Case C – 362/14, *Maximilian Schrems*, paragraph 70, on the "adequate level of protection", which states: "*It is true that neither Article 25(2) of Directive 95/46 nor any other provision of the directive contains a definition of the concept of an adequate level of protection*". In particular, Article 25(2) does no more than state that the adequacy of the level of protection afforded by a third country "*shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations*" and lists, on a non-exhaustive basis, the circumstances to which consideration must be given when carrying out such an assessment.

[28] See Document: "Transfers of personal data to third countries: applying Articles 25 and 26 of the EU Data Protection Directive", document setting out the criteria for assessing the adequate level of protection, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_es.pd. The Directive referred to in the document is Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, which has been replaced by Regulation 2016/679.

This provision (Article 36) also states that, when assessing the adequacy of data protection the Commission shall take into account, in addition to the criteria already set out, the access of public authorities to personal data, as well as the implementation of such legislation, data protection, professional rules and security measures.[29]

It should be noted that the Directive also emphasizes the adequacy of data protection on the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject. This supervisory authority shall ensure and enforce compliance with data protection rules [Directive, Article 36 (b)].

In order to complete the demand for the adequacy of the level of protection required to enable the Commission to authorise the transfer of personal data to a third country or international organisations, in accordance with Article 36 (c), it is necessary to require international commitments entered into either by a third country or international organisation, or other obligations arising from legally binding conventions or instruments as well as from their participation in multilateral or regional systems, particularly in relation to the protection of personal data. In this respect, it should be noted that the Commission shall take into account its accession to the above-mentioned Council of Europe Convention on 28 January 1981 and its additional Protocol.[30]

IV. Exceptional data transfers in specific situations

In Article 37, the Directive foresees two cases in which the transfer of personal data to a third country or international organisation in the absence of an adequacy decision must be provided where:

a) There are adequate safeguards or, where they have provided appropriate safeguards for the protection of personal data in a binding instrument ensuring the protection of personal data (Article 37). Among these instruments, the Directive mentions, for example, legally binding bilateral agreements which have been concluded by Member States and implemented in their legal order and which could be enforced by data subjects or, as an alternative mechanism, that the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. It is right that the Directive, in its Recital (71) has included, in relation to legally binding bilateral agreements, the cooperation agreements concluded between Europol or Eurojust and third countries, which will undoubtedly contribute to an effective response in the fight against terrorism by allowing the exchange of personal data even in the absence of an adequate level of protection in the framework of a judicial investigation.

b) Even if there is no prior authorisation by the Commission to carry out the transfer of data to a third country or an international organisation, either in the absence of an adequacy protection or of the appropriate safeguards referred to in the Directive, such transfer (Article 38) may expressly be carried out in the following cases: a) to protect the vital interests of the data subject or another person; b) to safeguard the legitimate interests of the data subject, where the law of the Member State transferring the personal data so provides; c) when it is essential to prevent an immediate and serious threat to the public security of a Member State or a third country; d) when the transfer is necessary in individual cases for prevention purposes; (e) when the transfer

[29] Judgment of the EU Court of Justice of 6 October 2015, Case C-362/14.
[30] See Article 12 of Council of Europe Convention 108 of 1981.

is necessary in individual cases for the establishment, exercise or defence of legal claims in relation to prevention, investigation, detection or prosecution of a criminal offence or the execution of a specific penalty. Exceptions to this must be very restrictive, exclusively for the cases referred to in the aforementioned article.

V. Independent supervisory authorities

Chapter VI, Articles 41 to 49, "Independent supervisory authorities", expressly states that each Member State shall provide for one or more independent public authorities to be responsible for monitoring *"the application of this Directive, in order to protect the fundamental rights and freedoms of natural persons in relation to processing of personal data..."*, which is reaffirmed in Recital (75). Such a supervisory authority should be set in accordance with Regulation (EU) 2016/679 [Article 41(3)], which expressly states that the supervisory authority established under that Regulation may be the supervisory authority in the processing of personal data for the purposes of prevention, investigation or prosecution of criminal offences or sanctions (Recital 76).

Article 46 of the Directive lays down a series of functions to be performed by the supervisory authority, including that of informing all data subjects of the exercise of their rights, promoting the awareness of data controllers and processors of their obligations and advising the national Parliament, the Government and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing. It is also assigned the role of cooperating with other supervisory authorities by sharing information and providing mutual assistance with a view to ensuring the consistency of application of this Directive.

At the same time, the Directive mentions the role of the supervisory authorities in assessing the appropriate level of protection. Thus, Article 38(1) of the Directive, as explained above, provides that, in the absence of an adequacy decision or appropriate safeguards, transfers of data to third countries may take place only under the requirements expressly provided for in paragraph (1), which are to be interpreted restrictively. Furthermore, such transfers *"shall be documented and the documentation shall be made available to the supervisory authority on request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred"*.

In turn, Article 39(3) of the Directive provides that, in cases of data transfer to specific recipients established in third countries *"the transferring competent authority shall inform the supervisory authority about transfers made under this Article"*.

Currently, concerning the Spanish legal order and as a consequence of the transposition of Regulation (EU) 2016/679, the independent supervisory authority lies with the Data Protection Agency, regulated by Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights.[31] In Title VII: "Data Protection Authority", Chapter I, Data Protection Agency is defined as an administrative authority, independent of State level (Article 44) and its action should be subject to the provisions of Regulation (EU) 2016/679. Its functions include supervision of the application of Organic Law 3/2018 as well as of the Regulation.

It should be noted that this is an administrative body with no functions concerning prevention and investigation of criminal offences or criminal sanctions. Therefore,

[31] BOE (Spanish Official Journal) No. 294, 6 December 2018

as far as the Spanish legal system is concerned, it will be necessary to wait for the transposition of Directive 2016/680 to see whether new tasks are granted to this body, which cover the content of the Directive itself, or, on the contrary, it will proceed to create another body to assume these tasks, thus responding to the provisions of Article 41 (3) "*Member States may provide for a supervisory authority established under Regulation (EU) 2016/679 to be the supervisory authority referred to in this Directive and to assume responsibility for the tasks of the supervisory authority to be established under with paragraph 1 of this Article*".