COrruption Risk Indicators in Emergency

Co-funded by the European Union

WORKING PAPER ON PUBLIC DATA AVAILABILITY AND ITS LIMITS: DATA PROTECTION & PRIVACY

Agustí Cerrillo (UOC)
Blanca Torrubia (UOC)
Mònica Vilasau (UOC)

Grant Agreement number: 101038790 — CO.R.E — ISFP-2020-AG-CORRUPT

This document was funded by the European Union's Internal Security Fund — Police.

1. Introduction

The *WP 1 on public data availability, interoperability and reusability* discusses the need to guarantee available information to be complete and thereby requiring public authorities (PAs) to ensure all relevant information is available to the public in general, and to the personnel representing contracting bodies including tenderers and contractors in particular making the interested parties able to obtain a full understanding of their activity.

This requires the information to be complete, i.e., containing all aspects associated with the life cycle of contracts and everyone who participates in them.

However, in certain circumstances potentially useful information for this purpose might not be provided when its dissemination could harm assets or rights specifically protected by current regulations (e.g., personal data, confidentiality of information, intellectual property and public safety). On this issue, PAs need to consider whether the information should be made transparent.

In particular, the objective of this WP 2 is to analyse how personal data protection could pose a limit to data availability and therefore a barrier to automated data analysis for the prevention and fight against corruption in emergency situations. In this regard, it should be borne in mind that Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information reiterates that the directive does not affect the protection of individuals with regard to the processing of personal data under Union and national law (recital 52).

Thus, to ascertain what personal data can be used and re-used to prevent and combat corruption, they first need to be anonymised or the data controller must comply with data protection regulations.

The following pages will examine the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR) to understand the principles governing any data processing that includes personal data. To illustrate the analysis specifically with regard to data that could be subject to analysis for the prevention of corruption (e.g. data on ownership of certain assets and companies), the following pages also include a specific study of Spanish legislation, which will serve as a case study.

This WP is organised into four sections. The first section analyses the principles of data protection in art. 5 of the GDPR. Next, the basis for data protection is examined and its impact on the fight against corruption is assessed. The third section focusses on reuse of personal data available in public records for the fight against corruption. In particular this latter section analyses access to and reuse of personal data held in the Civil Register, the Property Register and the Company Register. Finally, the WP concludes with a section on conclusions and recommendations.

2. The principles of data protection

Personal data are data that refer to an identified or identifiable natural person (art. 4.1 GDPR). Given this precept, an initial issue to note is that information regarding legal persons is expressly excluded from the scope of application of this regulation (art. 1.1 GDPR).

Processing personal information is subject to the GDPR. In particular all data processing should take into account the data protection principles in article 5 of the GDPR. These principles provide the ultimate interpretation to determine (or help determine) whether a given form of processing is possible.

The data protection principles not only affect the data controller (DC), but also everyone else involved in the processing. They are applicable to all people and organisations carrying out data processing.

A brief reference to the principles of data protection is given below:

2.1 Principle of 'lawfulness, fairness and transparency'

According to article 5.1.a of the GDPR, personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

As stated in recital 39, this means that it should be perfectly clear to natural persons that their personal data are being collected, used, consulted or processed in some other way, and the extent to which these data are or will be processed.

The principle of transparency requires all information and communication regarding data processing to be easily accessible and easy to understand, using clear and simple language. The principle of transparency is not only a principle, but also a right in arts. 12 to 14 of the GDPR.

The principal of lawfulness is developed in article 6 of the GDPR. This principle regulates the situations that enable, or permit, data processing. In the context of the EU, data cannot be processed if there is no authorisation, or legal basis, as discussed below.

Lawfulness, fairness and transparency are highly interconnected, especially the latter two. In particular, information must be provided on the identity of the DC and their purposes; in short, what they are going to do with the data.

2.2 Principle of 'purpose limitation'

Article 5.1 of the GDPR states that personal data may be collected for specific, explicit and legitimate purposes, and shall not be subsequently processed in a manner incompatible with these purposes. In accordance with article 89, section 1, further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes.

Recital 50 states that processing of personal data for purposes other than those for which the personal data were initially collected should only be allowed where compatible with the purposes for which they were initially collected.

2.3 Principle of 'data minimisation'

Article 5.1.c of the GDPR states that the personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation").

This means that processing personal data should first be assessed as to whether it is really necessary. If they must be processed, this processing should only be that which is essential for the desired purpose.

The minimisation principle should be related to data storage. Thus, a limitation on the storage period is established.

There are also exceptions to this data storage limit requirement, such as processing for archiving purposes in the public interest.

2.4 Principle of 'accuracy'

Article 5.1.d of the GDPR states that personal data shall be accurate and, if necessary, updated; all reasonable measures will be adopted to erase or rectify without delay personal data that are inaccurate with regard to the purposes for which they are processed.

Data must be accurate and up to date. Otherwise, they must be rectified or erased. This also has a bearing on the duty of the DC to inform the data recipients that the data have been rectified/erased. This is established in article 19 of the GDPR in relation to exercising the right to erasure (art. 17 GDPR).

With regard to the principle of accuracy, official data rectification and updating may in certain cases raise problems with confirming and accrediting the consent of the data subject.

2.5 The principle of 'storage limitation'

Article 5.1.e of the GDPR states that personal data shall be kept in a form that permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as they are processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with article 89, section 1 subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

The principle of data minimisation, with regard to the data storage period, should be borne in mind.

Specifically, the information clauses should include the period for which the personal data will be stored or, if that is not possible, the criteria used to determine the period (arts. 13.2.a and 14.2.a of the GDPR).

2.6 Principle of 'integrity and confidentiality'

Article 5.1.f of the GDPR states that the personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

One of the novel aspects the GDPR introduces is the new orientation given to data security, adopting a risk responsibility approach, which may be seen as a cross-cutting principle to all data processing.

The measures adopted to tackle possible risks must consider the nature, context and purposes of processing, and the risk such processing might pose to people's rights and freedoms.

In short, appropriate security against unauthorised or unlawful processing and accidental loss, destruction or damage must be guaranteed through technical or organisational measures.

The novel aspect is not the security obligations, but the instruments to make them effective. There are three main instruments: assessment of the risks to be tackled when starting processing; implementation of appropriate technical and organisational measures and notification of security violations.

2.7 Principle of accountability

Article 5.2 GDPR states that "the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1". This is the principle known as accountability.

Based on such accountability, organisations must be aware of what information they process and for what purpose, and must plan and design how to comply with the GDPR standards. In addition, they must accredit their appropriate compliance with the regulation when required.

3. Basis for data protection and its impact on the fight against corruption

3.1 The starting point for permission to process personal data

As indicated in the context of the EU, processing personal data requires a legal basis, as indicated by the principle of lawfulness (art. 5.1.a GDPR). Information regarding natural persons cannot be used indiscriminately; there must be a legal basis for doing so. Such legal bases are contained in art. 6.1 of the GDPR.

In analysing the different instances, an initial distinction will be made depending on whether the DC is a PA or a subject other than a PA.

3.2 Cases when the DC is a PA.

In such cases, personal data for processing can come from two sources: a PA (the PA using the data from another PA) or subjects other than PAs.

A. When the data are not held by the PA

If the data are not held by the PA, the different legal bases included in art. 6.1 GDPR need to be examined. According to this precept, processing is lawful if it complies with at least one of the conditions considered in the article.

First of all, one sees that art. 6.1.a of the GDPR refers to the data subject's consent. According to art. 4.11 of the GDPR, this consent must meet certain criteria for processing to be legitimate. In effect, consent must be a "freely given, specific, informed and unambiguous indication of the data subject's wishes by which

he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". The requirement that raises major questions in relation to PAs is whether consent in relations between the PA and data subject can be considered as freely given. To the extent that it cannot be considered free because it is given a situation of imbalance, the consent is not adequate for processing personal data. According to the Article 29 Working Party "consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences (e.g. substantial extra costs) if he/she does not consent. Consent will not be free in cases where there is any element of compulsion, pressure or inability to exercise free will".[1] Along these lines, recital 43 of the GDPR states that consent "should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation".

Secondly, art. 6.1.b of the GDPR refers to the case in which processing "is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract". Although one can find cases of contractual relations with PAs in which certain information is required from the data subject to finalise and perform the contract, this is not the case for processing carried out in the context of the C.O.R.E project. Hence this would not be a generally applicable legal basis.

Thirdly, art. 6.1.c of the GDPR considers processing required to *comply with a legal obligation* applicable to the DC as a legal basis. This could be a legal basis PAs might use for data processing.

Fourthly, art. 6.1.d of the GDPR considers processing when necessary to protect the vital interests of the data subject or of another natural person. Once again, this does not see appear to be a legal basis applicable to processing aimed at preventing or combating corruption.

Fifthly, art. 6.1.e of the GDPR states that processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the DC is a legal basis. Below we analyse whether this could be an applicable legal basis for processing to prevent and combat corruption in emergency contracts.

Finally, in sixth place, art. 6.1.f of the GDPR states that "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child".

However, the instance in art. 6.1.f of the GDPR must be ruled out immediately, as the precept itself establishes that "Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks".

Below we analyse the instances in art. 6.1.c and 6.1.e of the GDPR, which are the principles that permit processing by PAs. It should be borne in mind that member states can introduce more specific provisions to adapt the application of such precepts (art. 6.2 GDPR). Also highly relevant is art. 6.3 of the GDPR, which states that the basis for processing indicated in these sections should be established in Union Law or the Laws of the member states applicable to the DC. In the case of Spain, this precept is implemented by Organic Law 3/2018, of 5 December, on the Protection of Personal Data and the Guarantee of Digital Rights (LOPDGDD) which expressly stipulates the demand for a regulation with the force of law (art. 8 LOPDGDD). According to this precept, this regulation could determine the general conditions for processing, the types of data that are

[1] Article 29 Working Party (2017). *Directives on consent in the sense of Regulation (EU) 2016/679 adopted on 28 November 2017 and last revised and adopted on 10 April 2018*.

subject to it, the transfers acceptable as a consequence of compliance with the legal obligation and the special conditions for processing.

B. Sharing data between PAs

The reuse of data for the prevention or detection of cases of corruption in public contracts in times of emergency occasionally requires PAs to exchange data with one another.[2] Data held by one PA may be of use in analyses performed by other PAs to detect conflicts of interest or cases of corruption.

PAs can use electronic means to exchange data. Indeed, in some countries such as Spain, PAs and their agencies, public organisations and associated or dependent bodies are expected to use these media in relations with one another (article 3.2 Law 40/2015, of 1 October, on the public sector legal system, LRJSP).

For PAs to effectively exchange data with one another, the electronic media they use must be interoperable to ensure the information systems of the different PAs can truly interconnect and exchange information and the PAs share data.

Interoperability is the capacity of information systems and the procedures they facilitate to share data and facilitate information and knowledge exchange between them.[3] Interoperability permits PAs to communicate, interpret and exchange data. This means the data exchange must first be defined and share common standards. To do this, PAs have gradually adopted technical standards establishing the necessary protocols and criteria to ensure interoperability.

Along these lines, Europe has promoted the European Interoperability Framework which contains 47 recommendations for the design of interoperable digital services. In addition, member states have steadily adopted standards to ensure the interoperability of data and services provided by different PAs. For instance, in the case of Spain, the National Interoperability Scheme includes a set of criteria and recommendations regarding security storage and standardisation of information, formats and applications for PAs to take into account when making decisions on technology that ensure interoperability (article 156.1 LRJSP).[4]

For PAs to effectively exchange data with one another, the electronic media they use must also be secure. Similarly, they must also guarantee the confidentiality, integrity, traceability, authenticity, availability and storage of the data, information and services used by PA electronic media. To do this PAs acquire infrastructures that ensure these principles in accordance with the requirements established in current interoperability standards and criteria.

Finally, it should also be remembered that when the exchanged data are personal, the principles of the GDPR must also be guaranteed.

In effect, the exchange or communication of data between PAs is to all intents and purposes personal data processing (article 4.2 GDPR) so that any data exchange between PAs must comply with data protection regulations. In this regard, we should remember that personal data can only be communicated to a third

[2] Strictly speaking, when a PA uses the data from another PA, this is not a case of reuse as stated in Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the reuse of public sector information, which defines reuse as "the use by persons or legal entities of documents held by: a) public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the documents were produced, except for the exchange of documents between public sector bodies purely in pursuit of their public tasks" (art 2.11).

[3] Preamble to Royal Decree 4/2010, of 8 January, regulating the National Interoperability Scheme in the field of the Electronic Administration.

[4] The National Interoperability Scheme is included in Royal Decree 4/2010, of 8 January

party to comply with purposes directly related to the legitimate functions of the transferor and transferee and with the prior consent of the data subject.

When PAs exchange or communicate personal data, this must have an appropriate legal basis and processing must respect the principles governing all processing and comply with the rights recognised in the GDPR.

With regard to the legal bases legitimising data exchange between PAs, those most clearly applicable are:[5]

- processing is required to comply with a legal obligation applicable to the DC (c);
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the DC (e);
- processing is necessary for the purposes of the legitimate interests pursued by the DC (f).

One for the most common applications of data communication is establishing or confirming the accuracy of personal data held by another PA (e.g. address, national identity card number, or whether the person is a member of a single-parent or large family). With regard to this instance, communication could be conducted in line with articles 6.1.c and e of the GDPR.

In relation to the incidence of processing principles, in such processing it is important to bear in mind the scope of the principle of purpose limitation, in that data cannot be processed in a way that is incompatible with the purposes for which they were initially collected (art.5.1.b GDPR). The DC must analyse the purpose for which they were collected.

The principle of storage period limitation also requires identification of the data subject to last no longer than is necessary for the personal data processing purpose, except, for instance, when the personal data are stored for longer for archiving purposes in the public interest (art.5.1.e GDPR).

In the latter case, communication based on compliance with a task performed in the public interest or necessary in the exercise of official authority vested in the DC will require powers granted by a regulation with the force of law.

A specific instance of data communication is considered with regard to personal data processing carried out by organisations with powers in exercising the public statistics function. This communication is only considered compatible within article 6.1.e of the GDPR in cases where the statistics requiring the information is demanded by a regulation in European Union Law or is included in the legally stipulated statistical programming instruments.

Occasionally, electronic document exchange between PAs occurs in closed communication environments which ensure authentication and identification of the senders and recipients and also the integrity of the exchanged documents (as expressed, for instance, in Spain in art 44.1 LRJSP). The established conditions and guarantees must cover both accessing the closed environment and transferring the data, and must guarantee the security of the closed communication environment and the protection of the transferred personal data. When senders and recipients of electronic documents both belong to the same PA, this PA must specify the conditions and guarantees covering the document exchange in the closed environment. These conditions must specify the relation between the authorised senders and recipients and the nature of the data being exchanged. When senders and recipients belong to different PAs, the conditions and guarantees must be established by an agreement signed by both parties (art. 44.2 and 3 LRJSP).

[5] As stated above, the data subject's consent would not generally be an appropriate legal basis for communicating personal data between PAs.

C. The issue of sources accessible to the public

The GDPR does not consider that fact that data are available in a publicly accessible source as a legitimate basis for personal data processing.

Such a basis is not alien to European legislation. Indeed, Organic Law 15/1999, of 13 December on the Protection of Personal Data (LOPD) passed while Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data was still in force, considered an instance in which personal data could be processed, specifically if they were in publicly accessible sources, insofar as they were necessary to meet a legitimate interest.

In particular, art. 6.2 of the LOPD states that "Consent will not be required when the personal data [...] are in publicly accessible sources and their processing is necessary to meet a legitimate interest pursued by the file controller or by the third party to whom the data are communicated, insofar as it does not infringe the fundamental rights and freedoms of the interested party".

In addition, publicly accessible sources were defined as "files that can be viewed by anyone without impediment from limiting regulations or further requirement than the payment of a possible fee" (art. 3.j LOPD). In particular, the following are considered *exclusively* to be publicly accessible sources: electoral roll, telephone books in the terms stipulated in their specific regulations, and lists of members of professional groups that contain solely name, title, profession, activity, academic level, address and indication of group membership. Also considered as publicly accessible sources are official agendas and gazettes and the media.

Now, publicly accessible sources are not considered a legitimising mechanism in the GDPR, or, logically, in the LOPDGDD. There is only one reference to "publicly accessible sources", in art. 14.2.f of the GDPR. However, no definition is provided nor is there reference to the requirements for using the data.

D. The instance where the personal data are on the Internet

1. Information *not* provided by the data subject

On this point we need to ask whether information on the Internet, such as information on cases of corruption from news stories and newspaper archives, can be used. Such processing would be useful for tracing and indexing news stories about previous cases of corruption to raise the alarm.

In particular, in what instances could such tracking or indexing be lawful?

In the case of PAs, as already highlighted, arts. 6.1.c and 6.1.e of the GDPR would be the applicable principles, requiring a regulation with the force or law to authorise such processing.

With regard to private parties, such as an NGO or other civil society organisations, who carry out such tracking, authorisation would come from legitimate interest (art. 6.1.f GDPR).

Recital 47 GDPR may also be relevant, specifically when it establishes that "The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned [...]".

Therefore, with a degree of caution, such legitimate interest could be claimed for processing data found on the Internet with the purpose of preventing corruption by the private individuals. However, the legitimate interest might not be sufficient basis to carry out general and automatic processing of all information found on the Internet, for cross-matching with information obtained from other databases.

Whatever the case, an impact assessment would have to be carried out and the rights involved carefully considered. In this impact assessment, the DC should explain and justify the reasons why, according to the DC, the intended processing would be permitted. Consultation with the competent data protection authority should also be considered.[6]

2. Information provided by the data subject

In this case, we need to analyse whether information on the Internet that the data subject has provided can be used, such as information the data subject posts on social media, websites and the general media.

Initially, art. 9.2.e of the GDPR would appear to be applicable when it states that "processing relates to personal data which are *manifestly made public* by the data subject".

However, the first potential objection to the use of this exception is that this precept does not fully include the basis that authorises data processing, where one of the legal bases in art. 6.1 of the GDPR is also required.

Along these lines, art. 9.2 of the GDPR should be interpreted in relation to the first section of the same article. Art. 9.1 GDPR establishes a general rule prohibiting certain types of processing that reveal ethnic or racial origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. After establishing this general prohibition, art. 9.2 GDPR provides a list of all the instances in which this prohibition may be "lifted". In particular, art. 9.2. states that "Paragraph 1 shall not apply if one of the following applies: [...]", including when the data subject has given their *explicit consent* to the processing of those personal data for *one or more specified purposes* (a), and processing relates to *personal data which are manifestly made public by the data subject* (e).

Whatever the case, despite the above, we will continue examining the possibility of invoking art. 9.2.e of the GDPR, which might be understood as an example of the bases in art. 6.1.a. However, the instance considered in art. 9.2.e refers more to an instance of tacit consent.

It is worth remembering the definition of consent in art. 4.11 of the GDPR: "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

[6] In this regard, the indications established in WP 217 of 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014 should be taken into account

The question is therefore does art. 9.2.e of the GDPR fall within the definition of consent in art. 4.11 of the GDPR? Is having published data on a social media network or a media outlet an unambiguous form of consent? Does it mean the data may be processed?

With regard to this issue, the following elements should be considered:

i. Initially, art. 6.1.a of the GDPR establishes that consent is for "one or more specific purposes". These purposes are known before processing is carried out. However, in the case of using data posted on social media, the purposes are known afterwards. According to art. 14 of the GDPR, the DC should communicate the information required by this principle.

ii. Arts. 6.1.a and 9.2.e, should be considered alongside art. 5.1, as it establishes the need for the *principle of purpose*. Thus, publishing photos and data on social media on fashion, for example, would not imply that these data can be used for another purpose, such as the fight against corruption.

iii. - However, the preliminary section of the civil code, especially art. 7.1, should be considered, where it states: "1. Right must be exercised in accordance with the demands of good faith.". This also stems from the principle that no-one can go against their own actions or against the trust generated in third parties due to the behaviour of a given subject.

The principle, the estoppel doctrine, is based on the need to protect good faith and trust, as well as appearances and stability in legal situations. Good faith is lacking when the result of one's own actions are contradicted, carrying out an ambiguous act to intentionally benefit from its dubious meaning, or a legal appearance is created which is later contradicted to the detriment of those who put their trust in it.

iv. In the sphere of personality rights, the subject's conduct is highly relevant, therefore a degree of importance must be given to their behaviour, in this case, their behaviour in the publication of photos, information about themselves and so on. Whether or not the subject is a public figure should also be considered. This is specified, for example, in Organic Law 1/1982 of 5 May, on the civil protection of the right to honour, personal and family intimacy and self-image (art. 2.1) which states that "civil protection of honour, intimacy and self-image shall be limited by laws and by social customs in line with the ambit that each person, by their own actions, reserves for themselves and their family".

Reuse of personal data published on social media

To conclude the assessment of the application of art. 9.2.e of the GDPR, it is worth including the sentence from the Spanish Constitutional Court 27/2020, of 24 February 2020.

The background to this sentence is the following:

A local newspaper published a news story on an event. A person, after attempting to murder their brother, committed suicide. The new story on the events occurring in a small city provided numerous details on the family of the murderer and suicide and also included a photo of the

injured brother. This photo had been taken from the subject's Facebook profile. The latter sued the newspaper for infringing the right to self-image.

The trial court and national court found the newspaper guilty and awarded damages to the victim. They judged that the plaintiff's photograph had been reproduced and publicised without his consent and the importance of the reported facts was insufficient to justify its inclusion in the report.

The Supreme Court partially upheld the newspaper's appeal. Although it considered the published information to be accurate and a newsworthy story, it ruled that the subject's right to self-image had been infringed because the photo had been taken from his Facebook profile. According to the Supreme Court "the fact that 'in the open account of an Internet social media network' the holder of the profile has 'posted' a photo of himself which is accessible to the general public does not authorise a third party to reproduce it in a media outlet without the holder's consent, because such an action cannot be considered a natural consequence of the accessible nature of the data and images in a public profile from an Internet social media network. The purpose of an open account on an Internet social media network is for the holder to communicate with third parties, provide these third parties with access to the content of the account and allow them to interact with the holder, but not to let them publish images of the account holder in the media". The Supreme Court stressed that publication on a social media network is not the equivalent of taking a picture in a public place and that "the right to freedom of information does not legitimise publication of the person's image without consent in a setting other than the one where the events took place, as it was not taken in the place of the events as a result of the event [...], but was obtained from his Facebook profile".

On appeal to the Constitutional Court, the appellant claimed that the image of the victim was neutral and respectful and was obtained from a publicly accessible source, insisting that publication on social media should be considered under the estoppel doctrine.

In its sentence, the Constitutional Court reiterated (Legal Basis 3) that "except for certain exceptions, no matter how much citizens voluntarily share personal data online, *they continue to possess their private sphere, which must remain separate from the millions of users of Internet social media networks, as long as they have not given their unequivocal consent* to being observed or having their image used and published".

According to the Constitutional Court, "The fact that private data circulate on Internet social media networks does not mean, in a more absolute way, as the appellant seems to defend, that the private has become public, given that the digital environment is not comparable to the concept of a 'public place', as defined in Organic Law 1/1982, nor can it be affirmed that citizens of the digital society have lost or waived the rights protected in art. 18 CE. Individuals who communicate over a digital environment and benefit from the opportunities provided by the Web 2.0 cannot, for this reason alone, lose their fundamental rights, whose ultimate purpose is the protection of personal dignity... Consequently, we reiterate that, unless there is an unequivocal authorisation for taking, reproducing or publishing the image from its owner, interference with the fundamental right to self-image must necessarily be justified by the prevailing public interest in having access to and publicising it" (Legal Basis 3).

According to the Constitutional Court, someone who posts an image on social media does so for others to see, and only consents to being observed in the chosen place. However, "[...] we cannot accept the premise adopted by the appellant, as the Facebook social network is characterised by the fact that its main objective is to facilitate and strengthen personal relations between its users. *In this instance the estoppel doctrine cannot be applied*, as it is based on the protection of trust and the principle of good faith, which imposes a duty of coherence and self-limits freedom of action when reasonable expectations have been created in the behaviour of others. In accordance with the habitual behaviour of users of Internet social media networks, especially those such as Facebook, it cannot be said that I.I.L., by publishing his photograph on his profile, was creating in the appellant editor (or any other print media) the certainty that he had authorised its reproduction in the newspaper as a victim of an event. Nor can it be affirmed that I.I.L.'s voluntary behaviour was the factor that could have induced the appellant to act in this way, since no type of personal relationship existed between the two as a result of the use of the social media network. Therefore, the reasoning offered in the contested judgement must be shared" (Legal Basis 4).

Thus, the Constitutional Court rejects the argument regarding the existence of authorisation by the image rights holder for its use by third parties through the mere fact of having published or "posted" the photo in their profile in Facebook, whose purpose is social interrelations with other users (Legal Basis 4).

Furthermore, the Constitutional Court rejects the idea that social media may be considered a "place open to the public in the sense of art. 8.2.a of Organic Law 1/1982. The issue in question is reduced to a consideration of whether publication without consent of an image of an anonymous person, i.e. someone who is not a public figure, but who suddenly and involuntarily acquires a role in a newsworthy event, in this case as the victim of a failed murder attempt by his brother who later committed suicide, was a legitimate intromission in his fundamental right to self-image (art 18.1 CE)" (Legal Basis 5).

Having expressed this legal precedent, the following general considerations may be drawn:

1. The type of user of social or other online media should be taken into account. That is to say, if the subject is considered a person with a high degree of online visibility, such behaviours can have consequences.

2. The purpose of the social media or online environment where the information has been published should be taken into account. For instance, if the social media network is related to leisure or work, it could be used for a similar purpose.

3. This consideration needs to be made case by case, which means its use cannot be generalised for carrying out general and automated mining of information published on the Internet and social media.

3.3 Instances where the DC is a subject other than a PA

In these cases, the legal bases that may be used are the data subject's consent and legitimate interest.

With regard to consent, the requirements of art. 4.11 of the GDPR need to be taken into account:

- free: art. 7. of the GDPR which states that conditional consent is not valid.
- specific: linked to the purpose limitation requirement.
- unambiguous: it cannot be derived from the subject's silence.
- informed: specified in the requirements of art. 13 and 14 of the LOPDGDD.

With regard to legitimate interest, we refer the discussion above.

4. The reuse of personal data available in public registries for the fight against corruption.

As analysed in WP1, the public authorities have large amounts of data in their power, the analysis of which can be hugely useful for detecting conflicts of interest and cases of corruption. This is the case with data related to the people involved in public tenders and the execution of contracts.

Knowledge and analysis of their personal, financial and business circles can be hugely useful to identify possible conflicts of interest.

Some of the useful data on public procurement is published in the Official Journal of the EU (TED). Complementarily information about public contracts, is published in web portals, databases or platforms of public contracts at the national, regional or local platforms.

Furthermore, there are some main sources of information related to the personal circle of a particular bidder or contractor which can be useful in the prevention and fight against corruption that are governed by specific rules.

This is the case of the Civil Registry, where facts and acts referring to identity, civil status and other personal circumstances that can reveal kinships are recorded.

Another source of useful information is the Land Registry where acts and contracts related to ownership and other beneficial rights over real estate are recorded or noted, knowledge of which may, for example, allow the identification of cases of unjust enrichment due to corrupt actions.

Last, a third source of useful information for the fight against corruption is the Commercial Registry where different acts related to businesspersons are recorded, such as business name and name, domicile, administrators, mergers, company dissolutions and liquidations, and annual accounts.

To carry out the analysis of the legal system of these data, in what follows we will focus on the existing regulation in Spain. This study must not only enable the identification of what can and cannot be done with these data, but it must also provide information on the limitations that may be encountered when reusing personal data related to the family ties of a contractor, their properties or the contracting company.

4.1 Data protection and contract notices, websites and platforms

Knowledge and analysis of personal, financial and business circles of people involved in public tenders and the execution of contracts can be hugely useful to identify possible conflicts of interest.

As it has been described in WP1, some of the useful data on public procurement is published in the Official Journal of the EU. When this information contains personal data, it has to follow GDPR principles. In this line, the Legal notice of the Tenders Electronic Daily (TED) published by the Official Journal of the EU states that:

Protection of your personal data: TED notices

Introduction

The European Commission (hereafter 'the Commission') is committed to protect your personal data and to respect your privacy. The Commission collects and further processes personal data pursuant to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (repealing Regulation (EC) No 45/2001).

This privacy statement explains the reason for the processing of your personal data, the way we collect, handle and ensure protection of all personal data provided, how that information is used and what rights you have in relation to your personal data. It also specifies the contact details of the responsible Data Controller with whom you may exercise your rights, the Data Protection Officer and the European Data Protection Supervisor.

The information in relation to processing operation "TED notices" undertaken by unit C.3 "TED and EU Public Procurement" of the Publications Office of the European Union is presented below.

Why and how do we process your personal data?

Purpose of the processing operation: Unit C.3 "TED and EU Public Procurement" of the Publications Office collects and uses your personal information when publishing calls for tender of contracting authorities (European Union institutions, bodies and agencies, public authorities in the European Member States or in some cases of third countries) with their contact details, as well as notices of tender awards to successful tenderers, with the tenderers' contact details, on the Tenders Electronic Daily website, http://ted.europa.eu. These contact details of the contracting authorities and successful tenderers are required for a correct operation of public procurement procedures and in some cases contain personal data. The contact details are also used by the TED service for communicating with the contracting authorities when necessary, and to send them the link to the published notices as proof of publication.

Your personal data will not be used for an automated decision-making including profiling.

On what legal ground(s) do we process your personal data

We process your personal data, because:

- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body;

and - processing is necessary for compliance with a legal obligation to which the controller is subject.

Additional legal bases for the processing:

Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union

Commission Implementing Regulation (EU) 2015/1986 of 11 November 2015 establishing standard forms for the publication of notices in the field of public procurement

Directive 2014/23/EU of the European Parliament and of the Council of 26 February 2014 on the award of concession contracts

Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement

Directive 2014/25/EU of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors

Decision 2009/496/EC, Euratom of the European Parliament, the Council, the Commission, the Court of Justice, the Court of Auditors, the European Economic and Social Committee and the Committee of the Regions of 26 June 2009 on the organisation and operation of the Publications Office of the European Union

In addition, laws applicable to specific sectors.

Which personal data do we collect and further process?

In order to carry out this processing operation unit C.3 "TED and EU Public Procurement" of the Publications Office collects the following categories of personal data:

Contract notices:

- Contact person (person's job title or the first name and last name),
- office address,
- work e-mail address,
- office telephone number,
- fax number.

Contract award notices:

- name of the contractor (entity or physical person in specific cases),
- contact person (person's job title or the first name and last name),
- office address,
- e-mail address,
- website,
- office phone number,
- fax number.

How long do we keep your personal data?

Unit C.3 "TED and EU Public Procurement" of the Publications Office only keeps your personal data for the time necessary to fulfil the purpose of collection or further processing, i.e. for ten years in the TED website. After this, the notices are archived for historical purposes, in a non-public internal archive.

How do we protect and safeguard your personal data?

All personal data in electronic format (e-mails, documents, databases, uploaded batches of data, etc.) are stored either on the servers of the European Commission or of its contractors. All processing operations are carried out pursuant to the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission.

The Commission's contractors are bound by a specific contractual clause for any processing operations of your data on behalf of the Commission, and by the confidentiality obligations deriving from the General Data Protection Regulation ('GDPR' Regulation (EU) 2016/679).

In order to protect your personal data, the Commission has put in place a number of technical and organisational measures in place. Technical measures include appropriate actions to address online security, risk of data loss, alteration of data or unauthorised access, taking into consideration the risk presented by the processing and the nature of the personal data being processed. Organisational measures include restricting access to the personal data solely to authorised persons with a legitimate need to know for the purposes of this processing operation.

Who has access to your personal data and to whom is it disclosed?

Access to your personal data is provided to the Commission staff responsible for carrying out this processing operation and to authorised staff, including the staff of a contractor, according to the "need to know" principle. Such staff abide by statutory, and when required, additional confidentiality agreements.

What are your rights and how can you exercise them?

You have specific rights as a 'data subject' under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access, rectify or erase your personal data and the right to restrict the processing of your personal data. Where applicable, you also have the right to object to the processing or the right to data portability.

You have the right to object to the processing of your personal data, which is lawfully carried out pursuant to Article 5(1)(a).

You can exercise your rights by contacting the Data Controller, or in case of conflict the Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor. Their contact information is given under Heading Contact information below.

Where you wish to exercise your rights in the context of one or several specific processing operations, please provide their description (i.e., their Record reference(s) as specified under Heading Where to find more detailed information? below) in your request.

Contact information

- The Data Controller

If you would like to exercise your rights under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact the Data Controller, unit C.3 "TED and EU Public Procurement" of the Publications Office, info@publications.europa.eu.

- The Data Protection Officer (DPO) of the Commission

You may contact the Data Protection Officer (DATA-PROTECTION-OFFICER@ec.europa.eu) with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725.

- The European Data Protection Supervisor (EDPS)

You have the right to have recourse (i.e. you can lodge a complaint) to the European Data Protection Supervisor (edps@edps.europa.eu) if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by the Data Controller.

Where to find more detailed information?

The Commission Data Protection Officer (DPO) publishes the register of all processing operations on personal data by the Commission, which have been documented and notified to him. You may access the register via the following link: http://ec.europa.eu/dpo-register.

This specific processing operation has been included in the DPO's public register with the following Record reference: DPR-EC-00453.

Table: Legal Notice TED

Complementarily information about public contracts, is published in web portals, databases or platforms of public contracts at the national, regional or local platforms.

These websites and databases also have to follow GDPR and national regulation on personal data.

4.2 The Civil Registry

A. General framework

According to article 2.3 of LOPDGDD, processing derived from the Civil Registry, the Land Registry, and the Commercial Registry will be governed by their specific legislation, and additionally by the provisions of the GDPR and in the LOPDGDD.

As provided for in the Preamble of Law 20/2011, of 21 June, of the Civil Registry, the Civil Registry is conceived as a unique database and an electronic register, in which electronic entries are made, information is organised and the facts and acts concerning civil statuses are born witness to. From this conception, the use of new technologies and electronic signature are incorporated.

However, the electronic nature of the Civil Registry does not alter the guarantee of privacy of the data contained in it. Although the Civil Registry is excluded from the area of application of Organic Law 15/1999, of 13 December, on the Protection of Personal Data[7], special attention is paid to these data given that they contain information that affects the individual's private sphere. The relevant point is that the protected data belong solely to their owner and it is they who can authorise that they can be provided to third parties. (Preamble to Law, IV)

From the outset, it is important to remember that the Civil Registry is a public registry dependent on the Ministry of Justice (art. 2.1 CRL).

The Civil Registry is electronic and the data is subject to automated processing and integrated into a unique database whose structure, organisation and operation come under the competence of the Ministry of Justice, in accordance with the present Law and its implementing regulations (art. 3.2 CRL)

The facts and acts referring to the identity, civil status and other circumstances of the person have access to the Civil Registry (art. 4 CRL). This precept means implies a relationship between those who can be recorded.

B. Access to the Civil Registry

Before the Civil Registry, people have the right to access the information they request about the content of the Registry, with the limitations provided for in the Civil Registry itself (art. 11.c CRL) and in terms of "privacy in relation to especially protected data subject to a restricted information system" (art. 11.e CRL).

The exercise of these rights must be carried out in view of the operating principles of the Civil Registry (arts. 13 and 19 CRL).

Specifically, art. 15 governs the principle of information, although its specificity will depend on whether the person accessing it is a public official or a private individual.

i. regarding public administrations (art. 15.2 and art. 80.1 CRL)

The public administrations and civil servants can access the data contained in the Civil Registry in the course of their duties and under their own responsibility.

[7] Currently, this reference must be understood as referring to OL 3/2018, LOPDGDD.

According to the provisions of art. 80.1.1ª CRL, on access by public administrations and civil servants, "The data contained in the Civil Registry can also be made known by means of the special procedures agreed by the Directorate General of Registries and Notaries, when the information must be supplied periodically and in an automated way to fulfil public purposes, […] ".

Therefore, this regular and automated access requires a specific agreement. It is understood that this access may be granted when it is in the course of performing the duties that correspond to the public administrations. This will require an enabling provision in accordance with the provisions of art. 8 LOPDGDD.

ii. regarding private individuals (art. 15.3 CRL)

When other individuals request information (persons other than public officials): provided that (a) the identity of the applicant is verified (b) there is a legitimate interest.

Third parties can also access the content of the data stored in the Civil Registry when there is authorisation (consent) from the owner of the data.

In any case, and regardless of whether the data are requested by the public administrations or a private individual, it must be remembered that specially protected data are exempt from the general information system, which will be subject to the restricted access system, ex articles. 83 and 84 CRL (art. 15.4 CRL). In this case, justifiable grounds must be given to be able to access these data.

- Regarding information about the affected party related to requests made for registered data related to their person, in other words access, this information does not have to be provided to the interested party when the registration/communication of these data is expressly established by law (Recital 73, GDPR)

- The person in charge of the Civil Registry, as the person responsible for the file, must decide on matters of compliance with the principles, obligations and exercise of rights. They are obligated to store the information about the subjects that have accessed the register and to facilitate, if so requested by the interested parties, the recorded information, under the terms provided for in the CRL.

C. Posterior use of the data

The use to which the registered data may be put by the third parties that have accessed the data must be exclusively limited to the legitimate interest expressed, in the basis of which access to the content of the Civil Registry was granted.

The data cannot be used for purposes other than those alluded to in the application to access the Civil Registry (Limitation of purpose principle, art. 5 GDPR).

Use of the data for purposes other than those that legitimised access is only possible if: (a) the consent of the affected party has been given; (b) there is a legal authorisation; or (c) the existence of a legitimate interest can be claimed.

Exceptionally, the transfer of registry data is allowed when the information is going to be used for purposes of family, history and scientific investigation.

D. De facto situations

De facto situations such as common-law couples or the possession of status (regarding filiation) will not be accepted in the Civil Registry.

One must consider, then, whether obtaining, on a regular basis, the data contained in the Civil Registry concerning a specific event, such as a marriage, means a discrimination (due to it being recorded) with respect to relationships that by their nature do not have access to the Civil Registry.

4.3 The Land Registry

The object of the Land Registry is the publication of certain property rights, specifically the registration or annotation of acts and contracts related to ownership and other beneficial rights over real estate (art. 605 CC).

The principle of formal publication is understood as the opening of the Registry to all those who want to know its content and who manifest an interest worthy of protection. This is what the Civil Code provides for when it states that "The Land Registry will be public for those that have a stated interest in knowing the status of real estate or of annotated or registered beneficial rights" (art. 607, CC). In the same line, the Mortgage Act (MA) provides that ""The Registries will be public for those who have a known interest in ascertaining the status of registered real estate or beneficial rights. Interest will be presumed for all public authorities, employees and civil servants who are acting by virtue of office or official position" (art. 221 MA).

A. What public information is contained in the Land Registry?

The Land Registry publishes acts and contracts related to ownership and other beneficial rights over real estate, and given that these acts and legal businesses refer to natural persons the registry is also involved in the publication of personal data.

Article 9 MA establishes that, "The actual page of each property will necessarily incorporate its unique registry code." The entries in the register will contain details of the circumstances *related to the subject*, object and content of the registrable rights pursuant to the title deed and the entries in the registry, previously classified by the registrar. To this end, the entry will contain the following details:

e) "The natural or legal person in whose favour the entry is made]...".

f) "The person from whom the property or rights that must be registered have just come".

In relation to this precept, art. 51 of the Mortgage Regulations (MR) provides that the person in whose favour the registration is being made and the person from whom the property or right that is being registered has come, are determined according to the following rules:

a) If they are natural persons, the recorded information will be the name and surname; the national identity document; whether they are of legal age and, if not, the age, specifying the cause of emancipation where relevant; if the subject is single, married, widowed, separated or divorced and, if married and this affects the act or contract being registered, then the present or future rights of the conjugal partnership, the matrimonial economic system and the name, surnames and address of the spouse; the nationality and civil residence of the subject if they are accredited or manifested; and the residence with the circumstances that specify this.

b) Also recorded, where relevant, are the circumstances of the legal or voluntary representation, the personal circumstances that identify the representative, the power of attorney or appointment conferred by the representation and, where appropriate, its entry in the corresponding registry.

In short, together with the beneficial owners, the personal data of the subject to which they refer (national identity document, civil status as married or single) are directly highlighted. Other information about the affected party can also be inferred (for example, sexual orientation based on the name of the spouse). The registry information highlights a person's real estate assets, their financial capacity and their level of debt.

B. The legal basis for the processing

If the entry in the registry is voluntary, we must not assume from this that the legal basis for processing is the consent of the affected party. MARTÍNEZ ESCRIBANO highlights this fact, indicating that the legal basis for processing is art. 6.1.e) GDPR: "The processing is necessary for fulfilling a mission carried out in the public interest or in the exercise of public powers vested in the controller". According to this author, "This public interest entrusted to the data controller, or in other words the registrar, is real estate legal certainty. Remember that legal certainty is enshrined in the Spanish Constitution as one of the basic principles of art. 9.3" [8].

MARTÍNEZ GARCÍA and MIQUEL LASSO DE LA VEGA argue in the same direction when they state that the Land Registry publishes data not by consent but because the law authorises the registry to do so. According to these authors: "If the purposes of publication are the registration institution's own, then the consent of the owner is not required since the entry is voluntary and person who registers does so with all the pursuant consequences"[9].

C. Interests in tension

There are two interests in tension in the access and reuse of data contained in the Land Registry: (1) the information inherent to the Land Registry (2) the protection of personal data and privacy.

[8] Martínez Escribano, Celia, La Protección de datos personales en el Registro de la Propiedad, Indret: Revista para el Análisis del Derecho, ISSN-e 1698-739X, Nº. 3, 2020, p. 9-10.

[9] MARTÍNEZ GARCÍA, Eduardo and MIQUEL LASSO DE LA VEGA, Carmen, "Tratamiento de los datos en los registros de la propiedad y mercantiles y de bienes muebles. La visión del registrador (Commentary on article 2.3 LOPDGDD)", in Commentaries (coord. Troncoso), p. 457-459.

Therefore, the form and scope with which this information is supplied is undoubtedly an issue that affects data protection.

D. Ways in which publication is provided in the land registry

The information contained in the registry can be made public in different ways:

(i) through the registrars showing the registry ledgers to people that have an interest in consulted them by means of a photocopy of the entries. The ledgers cannot be taken away from the office and suitable precautions must be taken to conserve them (art. 222.1 MA and art. 332.1 MR). If requested, this manifestation can also be carried out by telematic means when the consultation is being made by a public authority, employee or civil servant who is acting by virtue of office or status (art.222.10 MA).

(ii) by means of a non-certified extract or certification from the registry (art. 222.2 MA). This is the usual way of providing information to interested parties and favours a better protection of personal data, by communicating solely those data whose knowledge is necessary for adequate and sufficient registry publication.

E. Requisites for applying for/providing registry information: known interest

If the Land Registry is public this does not mean that indiscriminate knowledge of all its content is possible.

To this effect, certain circumstances must be evaluated. In particular, the alleged interest: a key issue in relation to data protection.

According to the provisions of art. 221 MA, "The registries will be public to those with a known interest in ascertaining…". The interest that is accredited must be stated in the applications for information (art. 222 bis.1 MA). This interest that must be expressed succinctly (art. 222 bis. 3 MA). Prove to the registrar that there is a legitimate interest in accessing the information (art. 332.3 MR). This interest is presumed in the case of public authorities, etc. (art. 221.2 MA). The registrar will qualify the interest in the sense that they must consider whether providing the information requested is justified or whether the request should be denied. This assessment by the registrar is what will determine which data/circumstances among those recorded on the page in the registry can be included and which not in the information provided (MARTÍNEZ ESCRIBANO, p. 16).

The ruling of the Supreme Court of 7 June 2001 (contentious-administrative chamber) highlights the need to state the cause and purpose of the consultation so that the registrar can qualify the existence of legitimate interest and also comply with data protection regulations[10].

According to ESCRIBANO, the fact of the existence of a legitimate interest that allows information to be provided means that exceptionality also concurs, ex art. 6.1.f) GDPR.

A key aspect is that the interest in accessing the registry information can be very variable, but is only protected if it is linked with the purpose of the registry. It must be tied to the registry's purpose. This purpose

[10] A consequence of legitimate interest for requesting information is the identification of the interested party who is requesting the information from the registry. This identification must be made using the National Identity Card (DNI).

is that of publishing **certain** information about property in the interest of legal certainly and, in particular, of the security of real estate legal transactions (MARTÍNEZ ESCRIBANO, p. 17). This aspect connects with the principle of purpose ex art. 5.1.b) GDPR.

As pointed out by MARTÍNEZ GARCÍA and MIQUEL LASSO DE LA VEGA, p. 458, **regarding legitimate interest**, this must be:

- Known, in the sense of accredited.
- Direct, in that the person requesting the information is the interested party, and if not there must be a person responsible (identifying who the agent is).
- Legitimate, in the sense of lawful and not contrary to the law.
- Proprietary: it is not any interest but a proprietary interest.

As discussed earlier, to be considered justified it is not sufficient to simply allege interest, but the registrar must be satisfied of the congruence of this interest with the rest of the data submitted to them when requesting the information, thus carrying out an analysis together with the rest of the circumstances contained in the application.

F. Massive data request

The massive data request deserves special mention The Instruction of 17 February 1998, of the Directorate General of Registries and Notaries (DGRN), refers to this.

This instruction establishes that:

Fifth.

1. The Land Registry and the Commercial Registry **will not issue the official information when the purpose of the request is its massive incorporation into databases**, parallel registries, for the exclusive purposes of marketing or resale, thereby not responding to any mandate by the party interested in the information.

2. Applications for **mass official information will be processed** if they meet some on the following requirements:

a) To comply with a **legal provision** that enables statistical studies to be carried out.

b) If the objective **fulfils a public interest such as performing sectoral studies or financial planning** by the Public Administrations, Public Law Corporations, or non-profit public or private institutions for these purposes.

c) If **deriving from a collaboration agreement** signed with the College of Land and Commercial Registrars of Spain, which is who, by regulation, is responsible for publishing statistics with reference to the databases of the Registries.

In all cases, the applicant will undertake in writing to the processing and publication of the data taking place by means of their aggregation, such that the right to intimacy and privacy is safeguarded. In line with this regulation, in the information they issue the Registrars **will state** that **the incorporation of the data into computer files and databases** for individualised **consultation by natural or legal persons is forbidden**, even when the source of information is expressed.

Regarding the last exception, contemplated in § Fifth.2 c) of this Instruction, some doctrinal sections are against this.

In this respect, MARTÍNEZ ESCRIBANO points out that "While the first two exceptions seem manageable, the third is quite incredulous, because it empowers the College of Registrars, which is not even a public administration, and in the entire absence of a legal basis to legitimise this action, to make collaboration agreements that involve the mass transfer of data. The College of Registrars accumulates a huge amount of data, and this is justified for purposes of real estate legal certainty. Furthermore, it can also produce statistics based on these data. However, I consider that the mass transfer of data cannot be understood as sufficiently legitimised by the fact that the College of Registrars has signed a collaboration agreement with an entity." p.18

To this effect, this author has reservations about the power granted to the College of Registrars, which is not even a public authority, and with no legal basis for this action, to make collaboration agreements that involve the mass transfer of data. According to this author, the mass transfer of data cannot be understood as sufficiently legitimised by signing an agreement, and this issue must be regulated by law. p.18

G. When information is provided

As mentioned above, in the registry information there are real legal data and personal data. When conducting the weighting assessment, the registrar must evaluate not only which strictly personal data can be communicated, but also which data of other types but associated with the person can be communicated.

The registrar must only make known the data that are strictly necessary as a requirement derived from the data protection system (minimisation of data). The registrar must conduct this weighting assessment on a case-by-case basis.

Therefore, the publication of official information cannot consist in merely photocopying or making a literal copy of entries (arts. 233 MA and 334 MR), without prejudice to the cases legally provided for concerning official certified copies and the literalness of certain elements in which the applicant is interested.

H. Criteria for Data Protection in the Land Registry: Assessment and Weighting

After verifying that it is a case where the information requested will be provided, the specific data that can be provided must be defined.

The current guidelines are set out in the DGRN Resolutions, which provide solutions for specific cases at a practical level. However, and precisely because they refer to specific cases, by their very nature they often do not provide general guidelines.

Although it is true that the casuistry given provides satisfactory answers to the problems posed and the task of the DGRN is positively evaluated, sufficient legal cover is lacking.

In relation to this issue, MARTÍNEZ ESCRIBANO says, " In my opinion, the assessment and weighting that the registrar must conduct must weigh real estate legal certainty, which is the purpose pursued with the registry and the information contained in it, with privacy, which is the interest protected by the data protection regulations", p. 21

I. The consultation of queries

This involves informing the owner of the property and rights recorded in the registry about the identity of the applicant requesting their publication. This is set out in the Instruction of 17 February1998, which indicates that official information requests must be archived so that the applicant can always be known. The owner according to the records has the right to know who is requesting information about their assets and why.

4.4 The Commercial Registry: data about companies, members of advisory committees, etc.

A. Introduction

The Commercial Registry is made up of the territorial Commercial Registries and the Central Commercial Registry.

The Central Commercial Registry is an official publication institution which, since 1 January 1990, allows access to the commercial information supplied by the Provincial Commercial Registries, once the data are organised and processed in accordance with art. 379 of the Commercial Registry Regulations[11].

In the area of the Commercial Registry, it is essential to determine the way in which the principles of official information and the protection of personal data are combined.

In this context, the "Rules on matters concerning personal data protection" published on the website of the Central Commercial Registry[12] are, by virtue of their content, also applicable to the commercial registries of the territories. Based on the provisions of Regulation (UE) 2016/679, on General Data Protection (RGPD) – whose application is supplementary[13]- these rules include the criteria to follow for data protection in relation to the entry of documents in the registry, the request for their publication, the exit of documents and invoicing.

[11] Shows art. 379 of the RRM: "The Central Commercial Registry has the following functions:

1) Filing and publication of the names of legal companies and entities.
2) Centralisation, organisation and merely informative publication of the data it receives from the territorial Commercial Registries.
3) Publication of the Commercial Registry's Official Gazette.
4) Oversees the Registry related to companies and entities that have transferred their domicile abroad without rescinding their Spanish nationality.
5) Communication of the data referred to in art. 14 of Regulation EC 2157/2001 of the Council, of 8 October, approving the Statute of the European Limited Society, to the Official Publications Office of the European Union".

[12] http://www.rmc.es/documentacion/publico/ContenedorDocumentoPublico.aspx?arch=RMC-%20Normas%20en%20materia%20de%20Protecci%C3%B3n%20de%20Datos%20de%20Car%C3%A1cter%20Personal.pdf

[13] Organic Law 3/2018, of 5 December, on Personal Data Protection and the guarantee of digital rights, states in its art. 2 (Area of application of Titles I to IX and articles 89 to 94, section 3: "Processing to which Regulation (EU) 2016/679 is not directly applicable, due to the activities it affects not being included in the area of application of EU Law, will be governed by the provisions of its specific legislation, should this exist, and additionally by the provisions of the aforementioned regulation and the organic law. Among other types of processing in this situation are the processing carried out under the organic legislation of the general electoral system, the processing carried out in the area of penal institutions, and the processing derived from the Civil Registry and the Land and Commercial Registries.

B. Entry of documents

Regarding the entry of documents and the application of the GDPR, the "Rules on matters concerning personal data protection" cover the information that must be included in requests related to personal data and the rights of access, amendment, elimination, opposition, limitation and portability of the interested parties established in the GDPR, and state that obtaining and processing data is an essential requirement for the services provision.

C. Requests for publication of information and data protection

Of special interest are the criteria applied in matters of requests for information, for the purposes of the GDPR. To this effect, the "Rules on matters concerning personal data protection" indicate that the following aspects are informed about:

"1. The personal data contained in the request will be processed, for which the registrar is responsible, and the use and purpose of the processing is expressly provided for in the registry regulations. The information contained therein will only be processed in the cases provided for by law and, where applicable, for the purpose of invoicing the requested services.

2. Pursuant to art. 6 of the Instruction of the Directorate General of Registries and Notaries, of February 17, 1998[14]*, the owner of the data is informed that the data will be transferred to satisfy the right of the owner of the property(s) or right(s) registered in the Registry to be informed, at their request, of the name or denomination and address of the natural or legal persons who have collected information regarding their person or assets.*

In the Instruction of 17 February 1998, based on the provisions of article 23.1 of the Commercial Code, the DGRN establishes that: "The Commercial Registry is public Publication of information will be made effective by certification of the content of the entries issued by the registrars or by a non-certified extract or copy of the entries and documents deposited in the Registry. Certification is the only means of reliably accrediting the content of the registry entries[15]", indicating that the formal publication of the registry entries, referring to both the Land Registry and the Commercial Registry, is the only legally established means of knowing the legal situation of real estate, companies and other registrable subjects.

The instruction recalls that formal publication of information is adapted to the following principles:

1. Legal publication

[14] Instruction 17 February 1998, of the Directorate General of Registries and Notaries, on general principles of official publication and action of the Land and Commercial registers vis-à-vis requests for mass data. Available in: https://www.boe.es/buscar/doc.php?id=BOE-A-1998-4619.

[15] The types of commercial certification available via the website are: (https://sede.registradores.org/site/mercantil): certification of a certain position; certification of validity and responsibilities; certification for the issuance of the electronic certificate of representation of a legal person; power of attorney certification; certification of articles of incorporation; board regulation certification; council regulation certification; certification of powers of the Managing Director; certificate of beneficial ownership.

The purpose of formal publication is to prove, legally and extralegally, the existence, extension and limits of the registered right and that its owner is the only one legitimately entitled to dispose of it (defensive and offensive effects), as well as to streamline legal transactions and provide certainty to contracting, making possible in the real estate and commercial sphere the principle of legal certainty enshrined in the Constitution (article 9).[16].

The requirements for access to the rights in the registry are rigorous in order to give registry pronouncements solidity. The requisites to control for the veracity and preciseness of the information provided must likewise be rigorous (otherwise confusion and legal insecurity would be generated among those who enter into contract on this basis), as well as to control its scope in relation to the interest of the applicant (which is presumed in the commercial sphere), all under the exclusive responsibility of the registrar, as owner of the Archive (articles 222, 227 and 233 MA, 332 and 335 of its Regulations, 23.1 of the Commercial Code, and 77 and 78 of the Commercial Registry Regulations).

2. Direct publicity

Knowledge of registry entries must be available to any interested party in an effective way and without the need to resort to the compulsory intervention of companies and professionals to obtain them, at an additional cost, without prejudice to the right of the interested party to do so voluntarily if they so wish. However, under no circumstances does the possibility of directly accessing official information mean that the Registrars' database can be accessed and the files potentially altered, manipulated, eliminated or changed, To this effect, the Land Registry and the Commercial Registry must adopt the technical and organisational measures necessary to guarantee the integrity of the data contained in their archives and to prevent their alteration, loss or destruction.

Direct publicity means celerity in obtaining the information requested, under the professional control of the registrar, who ensures its adequacy in terms of the registry entries (veracity of the information). This involves the need to incorporate new technologies into the registries so that formal publications can be issued in real time with the due guarantees. "Real time" must be "real legal time", exempt from insecurity (the mere theoretical possibility of the information being manipulated would generate a questioning of the trustworthiness, the legal veracity, of the system).

Royal Decree 158/2008, of 8 February, modified art. 384 of the Commercial Registry Regulation, which now establishes:

[16] Indicated by the Instruction of the DGRN of 1 February 1998: The Land Registries, the Commercial Registries, the Central Commercial Registry, the Registry of Sales in Instalments of Movable Property (to be integrated into the Registry of Movable Property), the Ship and Aircraft Registries, and the Movable Mortgage Registries and Non-Possessory Pledge are registries of legal value intended not only for the general dissemination of their content, but also to attribute to the registered rights their full effects, in favour of their owner and to make contracting with third parties more flexible and secure."

"1. The commercial registrars will send the data to which this regulation refers to the Central Commercial Registrar immediately after making the corresponding entry. The provisions of article 370 are exempt from this.

2. Likewise, the expressed remission will be recorded immediately by means of a note in the margin of the entry made.

3. Professional publication

The formal publication of registry entries cannot consist in providing indiscriminate knowledge of the assets of people or mass publication. Whoever may wish to obtain information on entries must certify to the registrar that they have a legitimate interest in doing so, in accordance with the meaning and function of the registration institution, although in the commercial field this interest is presumed.

The Instruction of February 17, 1998 recalls that the legal investigation of property and companies in our system reduced, for reasons of safety, effectiveness, efficiency and economy, to the mere request for formal publication, is to falsify the purpose attributed to it by the regulations. Therefore, the purposes of the registry are considered to be the legal investigation, in a broad sense, of property and finances (credit, solvency and responsibility), and strictly legal investigation aimed at contracting or filing legal actions (object, ownership, limitations, representation, etc.), but not the private investigation of the non-property related data contained in the registry, such that the registrar may only disclose the pertinent information if the rules on data protection are complied with (article 18.4 of the Constitution "habeas data", vid. STC 254/1993).

Agreement between the College of Land and Commercial Registrars of Spain and the Secretary of State for Security.

On 12 March 2020 (BOE no. 113, of 23 April 2020), the Secretary of State for Security (Directorate General of Police, GDP) and the College of Land and Commercial Registries of Spain signed an agreement which, through the Police Station of the Judicial Police of the National Police, allowed the GDP to access at no cost the information available in the Commercial Registries on natural persons who presume ownership of more than 25% of the social capital of an unlisted trading company (what is known as the beneficial ownership of a legal person). The Agreement signed will initially be for a period of 4 years and is the culmination of the commitment of registrars, with GDP support, to combat money laundering and terrorism funding.

This Agreement stems from the interest of the Police Station of the Judicial Police of the National Police in requesting, via the Internet and using the website of the Registrars of Spain, information contained in registries for use by the National Police Investigation Units in carrying out the tasks for which they are responsible, and especially in relation to compliance with the regulatory framework established by Law 10/2010, of 28 of April, on the prevention of money laundering and terrorism funding, and the Regulation of Law 10/2010, of 28 April, approved by

Royal Decree 304/2014, of 5 May. This Law also obliges Notaries and Registrars to collaborate in achieving these objectives (art. 2.1. n).

Without prejudice to other possible future programmed queries, the beneficial ownership consultation service will enable the Police Station of the Judicial Police to carry out three types of consultations structured around the invocation of three different services:

a. Information request service. Beneficial owners of a company On entering the NIF of a trading company and indicating the year to which the query refers, the service will return the information about the beneficial owners that appear in the competent Commercial Registry in the tax year indicated. Should there be no information about the beneficial owners in the tax year to which the query refers, the service will deliver the last information presented in previous tax years.
b. Information request service. Companies whose beneficial owner is a natural person: On entering a NIF, the interested party will be informed of the companies that the person whose NIF it is the beneficial owner of, be it as a beneficial owner with over 25% of the shares or as an equivalent beneficial owner.
c. Information request service. Companies in which the owner of the NIF appears in its chain of control as a beneficial owner: On entering a company NIF, the interested party will be informed of the companies in which the owner of the NIF appears as an intervening company in the control chain of a beneficial owner.

The information displayed by each of the three services will be consistent with the information deposited in the Commercial Registry at the time the query is made, based on the data declared by the company in the last annual accounts it presented or, where applicable, updated at a later time by submitting a new declaration.

The College undertakes to allow communication with the web server of the Land and Commercial Registries to make requests for registered information to the registrars by authorized users belonging to the General Police Station of the Judicial Police in the manner decided by the two parties.

Last, in the ninth clause of the Agreement, the parties pledge to maintain the confidentiality of all data and information provided by the other party and that concern carrying out the object of the Agreement. The parties must keep this information confidential and secret and not reveal it in any way, in whole or in part, to any natural or legal person that is not party to it, except in the cases and in the manner provided by law.

For its interpretation, the Registrar relies on the Collaboration Protocol between the Data Protection Agency and the Land and Commercial Registries of Spain (3 November1994)[17].

[17] Furthermore, with regard to the protection of the legal and economic interests of consumers (article 51 of the Constitution and article 1 of the Consumer and User Defence Law), the publication of registry information must be expressed clearly and simply, stating its legal value (graphic clarity, clarity of concepts, merely informative value: Vid. Instruction 5 February 1987, fifth rule). Obviously, only certification bears witness to the content of entries (articles 225 MA and 23.1 of the Commercial Code). These principles have been repeatedly accepted and highlighted by the DGRN. The GDP is obligated to use these data exclusively for its own purposes, and their incorporation into databases and automated files that may be subject to individual consultation by natural or legal persons is prohibited.

In view of the previously described principles, the instruction agrees on a series of criteria that include:

a) The Land and Commercial Registrars will, in all cases, make known the pertinent part of the content of the registry to persons who request it, either as a non-certified or a certified document, by professionally processing the information, expressing it clearly and simply and excluding any data that have no legal significance, effecting the possibility of publication without the need for intermediation.
b) Commercial Registrars will facilitate consultation of the data relating to the essential content of entries by the interested party by means of computer terminals, delivering a copy of what has been consulted to whoever has requested it, as a non-certified informative copy.
c) When consultation of the archived data has been made by telematic means, the Registrar must at all times ensure the impossibility of its manipulation and data theft. Accordingly, direct access by any means, be it physical or telematic, to the database contained in the Archives of the Land and Commercial Registrars is prohibited. The Registrars will take responsibility for their custody, integrity and conservation, impeding any external access to the networks during the telecommunication, or to the programmes and codified barriers.
d) Requests made by telematic means will be dealt with by immediately sending the registry information by email or by another means, provided that there is an instantaneous interruption between the computer link of the request and the response.
e) Intercommunication between Registrars via telematic networks will make use of cryptographic techniques.
f) The Central Commercial Registrars will technically impede direct access to its databases and will ensure that consultations are made company by company, authorising intercommunication by means of a specific agreement that includes the non-incorporation into a database belonging to the applicant, in accordance with the third final provision of the Order of 10 June 1987.
g) Land and Commercial Registrars must comply with the applicable regulations on personal data protection.
h) Requests for information about personal data with no financial relevance will be made together with an expression of the interest pursued, which must be in compliance with the purpose of the registry.
i) The Land Registry and the Commercial Registry will not issue the official publication when the purpose of the request is its massive incorporation into databases, parallel registries, for the exclusive purposes of marketing or resale, thereby not responding to any mandate by the party interested in the information.
j) Applications for mass official information will be processed if they meet some on the following requirements:
    - If it is to comply with a legal provision that enables statistical studies to be carried out.
    - If its objective fulfils a public interest such as performing sectoral studies or financial planning by the Public Administrations, Public Law Corporations, or non-profit public or private institutions for these purposes.
    - If they derive from a collaboration agreement signed with the College of Land and Commercial Registrars of Spain, which is who, by regulation, is responsible for publishing statistics with reference to the databases of the Registries.

    In all cases, the applicant will undertake in writing to the processing and publication of the data taking place by means of their aggregation, such that the right to intimacy and privacy is safeguarded. In line with this regulation, in the information they issue the Registrars will state that the incorporation of the data into computer files and databases for individualised consultation by natural or legal persons is forbidden, even when the source of information is expressed.

k) Requests for the publication of official information will be archived for a period of three years, such that who the applicant is, their address and their national identity number or tax identity number can be known.

Law 7/1998, of 13 April, on general conditions of contracting, re-wrote articles 222 of the MA, adding among other points, point number 6, which states that: "The Registrars, when qualifying the content of the registry entries, will inform and ensure compliance with the applicable regulations on the protection of personal data." The MA was then adapted to the data protection regulations by means of Royal Decree 1867/1998, of 4 September, which re-wrote, among other articles, article 332, thus incorporating the criteria contained in the Instruction of the DGRN of 17 February 1998[18].

D. Exit of documents

Regarding the exit of documents, the "Rules on matters of data protection" specify, for the purposes of the GDPR, the following information:

1º) In accordance with the provisions of the registry information publication requests, the personal data expressed in them have been and will be processed and incorporated into the Registry Ledgers and files, for which the Registrar is responsible, and the use and purpose of their processing are those stated and expressly provided for in the registry regulations, serving as a legitimising basis for this processing.

2º) In accordance with art. 6 of the Instruction of the Directorate General of Registries and Notaries, of February 17, 1998, the owner of the data is informed that the data will be transferred to comply with the right of the owner of the asset(s) or the right /s registered in the registry to be informed, at their request, of the name or denomination and address of the natural or legal persons who have collected information regarding their person or assets.

3º) The period for which the data will be kept will be determined in accordance with the criteria established in the registry legislation, the resolutions of the Directorate General of Registries and Notaries and collegiate instructions. Regarding invoicing for services, the periods for which the data will be kept will at all times be determined in accordance with the applicable fiscal and tax regulations. Notwithstanding, the Registry may keep the data for a longer period than that indicated by the regulatory criteria in cases where this is necessary due to the existence of responsibilities derived from the provision of the service.

4º) **The information made available to the applicant is for their exclusive use and is non-transferable and confidential and may only be used for the purpose for which the information was requested. The transmission or transfer of information by the user to any other person, even if free of charge, is prohibited**

This limitation regarding the object of the information, its confidential nature and its exclusive and non-transferable use is important, given that these characteristics make it unsuitable for reuse.

*5º) **In accordance with the Instruction of the Directorate General of Registries and Notaries, of 17 February 1988, the incorporation of the data contained in the registry information into computer files or***

[18] In relation to requests for the publication information, the "Rules on matters of data protection" establish that when the request is compatible with the specific legislation of the Register, the rights provided for in the GDPR are recognised for the interested party. Furthermore, it is established that the user can appeal to the Spanish Data Protection Agency (AEPD) or can contact the Registry's data protection representative.

databases for individualised consultation by natural or legal persons, even when the source of origin is stated, is prohibited.

This last limitation confirms the impossibility of making public any data which, despite having an financial content of interest, are protected by the regulations on data protection.

6º) Insofar as it is compatible with the specific regulation applicable to the Registry, the interested parties' rights of access, rectification, deletion, opposition, limitation and portability established in the aforementioned GDPR are recognised, and they are able to exercise them by writing to the address of the Registry.

Likewise, the user can make an appeal to the Spanish Data Protection Agency (AEPD): www.agpd.es. Without prejudice to the aforementioned, the interested party can contact the Registry's data protection representative in writing at dpo@corpme.es [19].

E. The Official Gazette of the Commercial Registry

The Official Gazette of the Commercial Registry (BORME) is the instrument through which the data registered in the Commercial Registry is published. The BORME is currently published in electronic format, which is recognised as having legal character and effectiveness and the same effects as the printed edition (art.2 of Royal Decree 1979/2008, of November 28, which regulates the electronic edition of the Official Gazette of the Commercial Registry).

The BORME is published in the electronic headquarters of the State Agency Official State Gazette and so is accessible through the Internet. Its consultation is open and free of cost

Royal Decree 1979/2008, of November 28, states that accessing the BORME will include the possibility of searching and examining its content, although it does not specify the scope of these options. Neither does it indicate that the data are published in open format to facilitate their reuse.

The opening of the Commercial Registry and the BORME

[19] Regarding invoicing, the "Rules on matters of data protection" indicate that:

"For the purposes of the General Data Protection Regulation 2016/679 of the European Parliament and of the Council, of April 27, 2016, the following aspects are recorded:

1º) The person responsible for processing is the Registrar, and the use and purpose of the processing is the invoicing of the requested services.

2º) When compatible with the specific legislation, the rights of access, rectification, deletion, opposition, limitation and portability of the interested party established in the aforementioned Regulation are recognised, and they are able to exercise them by writing to Registry at their address. Likewise, the user can direct an appeal to the Spanish Data Protection Agency (AEPD) www.agpd.es.

Notwithstanding the foregoing, the user can contact our Data Protection Representative by email at dpo@corpme.es.

3º) The period for which the data will be conserved will always be determined in accordance with the applicable fiscal and tax legislation.

In recent years, various campaigns have been promoted in Spain to push for the opening of the Commercial Registry and the BORME.

To this effect, in December 2020, the Pro-Access Coalition addressed the Government to demand the complete, free and open data publication of the Commercial Registry, including the data on owners and the structure

Regarding this issue, it is important to mention that the IV Open Government Plan has foreseen the improvement of access to the data contained in the Commercial Registry within the framework of the transposition of Directive (EU) 2019/1151 of the European Parliament and of the Council, of June 20, 2019, amending Directive (EU) 2017/1132 with regard to the use of digital tools and processes in the field of company law.

In addition to these actions, some IT activists have promoted projects to facilitate the reuse of the information published in the BORME.

LibreBORME is a project promoted by Pablo Castellano in which a platform has been developed that allows data published in the BORME to be automatically extracted and downloaded for subsequent reuse.[20] The project involves extracting the data contained in the PDF documents published in the BORME and creating a commercial database that is updated daily and currently contains more than 5 million records.[21] The platform integrates a search engine and a tool to find relationships between people and companies.

5. Conclusions and recommendations

5.1 Conclusions about the fundamentals of data protection and its impact on the fight against corruption

The conclusions regarding the fundamentals of data protection and its impact on the fight against corruption are:

I. When a public administration must process data that are not in its possession, the main legal bases that can be called upon and that will legitimise this processing are that the processing is necessary to comply with a legal obligation or with a mission carried out in the public interest or in the exercise of public powers (arts. 6.1.c) and 6.1.e) RGPD).
II. However, the legal basis of this processing must be established by the Law of the Union or the law of the Member States (art. 6.3 GDPR) In the case of Spain, this is stipulated in that it must be a regulation that is legally binding. Additionally, this regulation may determine the general conditions of the processing and the types of data subject to it, as well as the transfers of data that result from complying with the legal obligation. This regulation may also impose special

[20] https://pablog.me/blog/2015/02/que-es-libreborme/
[21] https://librebor.me/

conditions on the processing, among them the adoption of additional security measures (art. 8 LOPDGDD).

III. When the public administrations exchange or communicate personal data, this must also be based on the aforementioned legal bases.

IV. Since the legal bases listed in art. 6.1 GDPR are considered to be a "numerus clausus", it appears that the processing of data obtained from sources accessible to the public cannot be admitted without a specific legal basis legitimising this.

V. In certain circumstances, and with the appropriate precautions, legitimate interest could constitute an adequate basis for processing personal data found on the Internet, such as in the online press. Nonetheless, an impact assessment should be carried out, the rights involved should be properly weighted, and the competent Data Protection Authority appropriately consulted.

VI. The images published on a social network are disclosed in a specific context. This behaviour does not mean they can be removed from this context and published elsewhere. Social networks are "spaces" that have a specific purpose and the images published in them are displayed in this context. They are posted as a way for users to interact among themselves. Therefore, the behaviour related to posting on a social network cannot be equated (at least automatically) to unequivocal consent, nor can it be equated with one's own actions. In certain cases, personal data published on the Internet or on a social network can be used. However, in this respect, different parameters must be considered, including the behaviour developed by the subject themselves and by the social network in question. To some extent, the purpose of the processing would be determined by the purpose of the social network itself. Another factor to consider is the scope of dissemination of the social network and whether it is an open/closed social network.

VII. In conclusion, a generalised and indiscriminate use of the information posted on the Internet or on social networks cannot be made. Notwithstanding, if the information made public can be used, it would be based on an analysis of specific cases, on a weighting of the different elements pointed out. To this effect, each case must be examined on an individual basis. Therefore, a generalisable assumption that the information published on social networks can be used in any case cannot be made, and even less be subjected to automated processing.

5.2 Conclusions on the reuse of personal data available in public records for the fight against corruption

Regarding the reuse of personal data available in public records in the fight against corruption, the conclusions are:

I. First, with respect to the reuse of data recorded in the Civil Registry:

- The Civil Registry exclusively publishes data of a personal type. Some of them are especially protected. Although the information in this registry is declared, access to it is not indiscriminate. The public administrations can access its content provided it is to carry out their duties and it is under their own responsibility.
- Civil Registry data can be accessed periodically and automatically to fulfil public purposes through the special procedures agreed by the General Directorate of Registries and Notaries. However, this should be provided for in a regulation with force of Law.
- Regarding private subjects, the identity of the applicant must be stated and there must be a legitimate interest. Specially protected data will be subject to restricted access. Since a legitimate interest is required, enabling a massive and periodic consultation of the data contained in the Civil Registry is considered to be difficult
- The fact that it is personal data being processed, arising from natural persons, means that the principles of data protection must be especially considered. In particular, the principle that the data

will not be further processed in a manner incompatible with the purposes for which they were collected.

II. Second, with respect to the reuse of data recorded in the Land Registry:

- The principles of information must be combined with the privacy and data protection of the subject concerned. When requesting registry information, it must be borne in mind that there are rules as to what information in the registry there is access to and as to its publication.
- There are also some procedures. The subject must follow some steps and the legitimate interest of the subject who wants to access the content of the registry must be assessed.
- The subject must state what their interest is and the registrar must assess whether this alleged interest can be considered a legitimate interest.
- In response to this legitimate interest, the registrar will transfer certain information to the applicant. To this effect, a matter such as a sale prices can be provided in some instances and not in others. If the interested party wishes to obtain information to terminate an action on the grounds of injury, or to challenge a deed of distribution of estate, this information may likewise be transferred in some cases and not on others.
- Personal data are usually disclosed in requests for information, some of which are specially protected (sensitive) data. For example, providing information about the name of the spouse may involve revealing someone's sexual orientation (for example, same-sex marriage). In this case, for example, the registrar may only provide the information (and indicate) that the subject is married, without identifying the spouse.
- The registrar obviously carries out an evaluative task of the information that can be provide (selecting what is relevant in relation to the specific request).
- We consider that this communication of information (the cause that enables it) is covered in the case provided for in art. 6.1.e) GDPR. Even when a subject themselves delivers a public deed to the registry, and it is recorded there, it does not seem appropriate to defend that the basis of this registration is the consent of the affected subject, since the owner of the deed cannot decide what data must be registered.
- The relevance is that the communication of information will be delimited by the principle relating to the fundament of the information in the registry, which is none other than that of providing legal certainty, security of transfer, which is what has to be weighed against the right to privacy and data protection.
- This, then, is the object of the weighting activity: secure transfer versus the privacy and data protection of the affected party.
- Regarding providing mass information, this involves a clash of different aspects: allegation of interest and each specific case having to be assessed and weighed by the registrar. The ultimate reason for allowing the disclosure of information is that the request for data must be related to the purpose of the property registry, which is to publish ownership to provide legal certainty. Last, although the February 1998 Instruction allows agreements to be made with institutions, it is doubtful that a simple Instruction can cover this. The doctrine considers that a simple agreement between the registry and a certain entity would not be adequate coverage for the communication of information.
- Notwithstanding, this communication should be protected by Law.

III. Third, regarding the reuse of data recorded in the Commercial Registry:

- The Commercial Registry is a public registry. Publication of information is effected by certification of the content of entries, either by non-certified or certified copies of the documents deposited in the registry (official information). Certification is the only means of reliably accrediting the content of entries.
- Official information is adapted to the principles of:

  a) Legal information. The purpose of official information is to prove, legally and extralegally, the existence, extension and limits of the registered right and that its owner is the only one entitled to dispose of it (defensive and offensive effects), as well as to speed up legal transpositions and provide certainty to contracting, making the principle of legal certainty enshrined in article 9 of the Constitution possible in the real estate and commercial spheres.
  b) Direct information: knowledge of the registry entries must be available to any interested party, in an effective way, and without the need to resort to the compulsory intervention of companies or professionals to obtain it, at an added cost. Nonetheless, this does not mean that the registrars' databases can be directly accessed (such that the files can be altered, manipulated, deleted or varied).
  c) Professional information: the publication of official information contained in registry entries may not consist of providing indiscriminate knowledge of people's assets or mass information. Anyone who wishes to obtain information about an entry must prove to the registrar that they have a legitimate interest in it, in accordance with the significance and function of the registry as an institution, although in the commercial field interest is simply presumed.

- The information made available to the interested party is for their exclusive use and is non-transferable and confidential. It can only be used for the purpose for which it was requested, and the transmission or assignment of the information by the user to any other person is prohibited, even if it is done so at no cost.
- The incorporation of the data contained in the registry information into computer files or databases for individualized consultation by natural or legal persons, even when the source of origin is stated, is prohibited.
- The only data whose knowledge is accessible to any natural or legal person, whether or not they are an interested party, are those known through the BORME.

5.3 Final recommendations

In view of the above conclusions, some recommendations must be made for the purpose of facilitating the use and reuse of personal data on the personnel at the service of the contracting authorities, and on bidders and contractors, to prevent and fight against corruption in emergency contracting:

1. The first is to adopt a regulation either at European level or in each Member State -in which case the scope will be determined by state legislation- which explicitly regulates the processing of the personal data of the personnel at the service of the contracting authorities, and of bidders and contractors, and which may be implemented by integrity agencies and anti-corruption offices for the prevention and fight against corruption in emergency public procurement. This authorisation

will constitute a specification of the legal bases legitimising the processing provided for in the GDPR regarding fulfilling a mission carried out in the public interest, or in the exercise of the public powers conferred on the person responsible for the processing.

2. To adopt a regulation either at European level or in each Member State -in which case the scope will be determined by state legislation- which explicitly regulates the processing of the personal data of the personnel at the service of the contracting authorities, and of bidders and contractors, and which can guide the entities whose social objective is the prevention and fight against corruption. This authorisation will constitute a specification of the legal basis legitimising the processing provided for in the GDPR regarding satisfying legitimate interests pursued by the person responsible for the processing.

3. To design and facilitate the creation of platforms that organise the huge amount of data published by official gazettes and, in particular, the gazettes of commercial registries (for example, the BORME) with criteria that allow their reuse Furthermore, to this effect, these platforms must disseminate the data in open format.

4. To update the databases of the official registries and gazettes to include search criteria that facilitate the identification of data of a certain person and to be able to obtain data to cross-reference with other records.

5. To promote the interoperability of registry information between the different Member States to be able to locate all the information related to a particular natural or legal person.

6. To promote citizen participation in the reuse of data, safeguarding the principles of data protection.

7. To promote cooperation with organisations to facilitate the control of real estate or capital that is outside the state territory.