Abstract

• The concepts of ‘data controller’ and ‘data processor’ in the Data Protection Directive are not exhaustive. The Directive defines them by excluding certain criteria (e.g. determining the means and purposes of the data processing, and carrying it out on behalf of the data controller). Thus, entities that do not fulfil such legal requirements when processing data are excluded from the scope of those concepts, and are considered as part of a third group of those who are processing data.

• Moreover, Article 7 (f) of the Directive refers to ‘third parties to whom data are disclosed’ and provides descriptions that imply that this category is based on a different assumption to those relating to data controllers and data processors, and is applicable to anyone who carries out data processing as an essentially personal activity.

• Articles 11, 12, and 14 of the Directive also establish a legal status that exempts these ‘third parties’ from some obligations that data controllers must fulfil.

• This article analyses and endorses the existence of this third category and the legal issues and problems that arise when trying to subject anyone who processes data to the legal regime applicable to data controllers and processors.

Approach

The concept of ‘third party to whom data are disclosed’ in the Directive

The legal regime established under 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’¹ (the ‘Directive’), in respect of those who process personal data, is divided essentially into two subjective elements: the data controller and the data processor.

These two elements are defined on the basis of the circumstances in which the activities are respectively carried out and, therefore, a data controller ‘determines
the purposes and means of the processing of personal data’, while a data processor ‘processes personal data on behalf of the controller’ (Article 2 (d)² and (e)³ of the Directive).

However, as these two definitions are so restrictive and limited, the Directive accepts some data processing assumptions that fall outside the scope of those concepts because, as neither of them has a residual or expansive nature, practical cases may arise where it is not possible to define who is submitting the data to process either as a controller or as a processor.

The Directive does not define the data controller as a common, or general and supplementary figure, which would be applicable to those processing personal data. Rather than provide that a data controller must process personal data, either directly or indirectly, the Directive restricts the concept of this subjective element by means of a condition that excludes those who do not meet it. According to the definition, those who do not specify the purposes and means of processing cannot be considered as data controllers of the process, even if they materially develop the processing of personal data.

An entity must always be in charge of determining the means and purposes of the processing, that is, a data controller, but this entity does not necessarily have to process the data materially, so those processing the data can do so applying a concept that differs from that of the data controller. This occurs when those processing personal data do not determine the purposes and means, but apply the data to the purposes and means of processing determined by the data controller.

Needless to say, this assumption that data are processed according to the purposes and means determined by a third entity cannot be confused with the assumption of several entities that make complementary decisions to define the means and purposes of the processing (joint data controllers), since the assumption referred to in this article is based on an entity that takes no part in making this decision and, therefore, merely applies the data for the purposes and in accordance with the means determined by one or more entities. Therefore, the possibility regulated under the Directive, stating that several entities can jointly determine the purposes and means, cannot be applied to anyone who does not decide the means and purposes, given that the joint determination of purposes and means requires that those involved in this decision participate actively.

Ultimately, by applying the concept established by the Directive, if an entity does not determine the means and purposes of the processing, it can never be qualified as a data controller, or as a joint data controller. It is possible that the means and

² The term “controller” shall be used for the natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;
³ The term “processor” shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;
purposes of processing can be determined by legislation, but in such cases the relevant rule should also determine who the controller is.

Moreover, a data processor processes personal data on behalf of the controller. The key to this concept lies on the fact that processing is carried out on behalf of the controller, that is, assigning the outcome and the consequences resulting from data processing to the controller. Under these circumstances, any data processing carried out by the data processor is attributed to the data controller, as though the controller had carried it out directly. As a result, Article 17 of the Directive, regulating the figure of the processor, allows the data controller to decide whether to carry out data processing directly, or outsource this activity to a different company, which will act as data processor on behalf of the data controller.

Similarly, data processors will provide any service that makes it necessary, as an ancillary activity to that service, for personal data to be processed.

The Directive does not define the data processor as being separate from the role of the data controller, assigning the role of data processor to those carrying out the process without determining its purposes and means, but as a unique and perfectly defined role that materializes when data controllers, instead of carrying out data processing directly through their own means, request a third party to perform the processing on their behalf.

Since data processors act on behalf of controllers, they have no personal interest in the outcome of the process they carry out (except the economic interest relating to the compensation agreed with the controller for the services provided, and their liability for the quality of these services); in fact, if data processors had any personal interest in the purposes sought in data processing, they would lose their status as data processor because they would stop acting on behalf of the data controller to act on their own behalf, for their own interest and, therefore, would not fit the definition of data processor provided under the Directive.

By applying these concepts, there may well be entities or individuals carrying out data processing that, because they do not fall within the definition of these concepts, cannot be qualified either as data controllers or as data processors of data processing. This would occur if an entity carried out its own processing, thus fulfilling its own interests, without determining the purposes and means of the data processing.

This raises the problem of defining how this data processing is dealt with, the liabilities and conditions that may be required of this third category of entities that process personal data. The Directive offers several provisions that, in accordance with its literal wording, are applicable to data processing carried out by entities whose role does not fall within the definitions of data controller or data processor.
Delimiting the concept ‘A Third Party to whom Data are Disclosed’

Article 2 (f) of the Directive defines third parties as a party other than the data subject, the controller, the processor, or those who process the data under the controller’s or the processor’s authority.

This concept is normally used in civil law to describe a subject that is not part of an entity or part of an agreement.

The limited rules referring to third parties in civil law focus on the possible effects that an agreement, a rule, or a human action could have on third parties. The most of those rules preserve their interests using the expression ‘without detriment to third parties’, as a limitation on the legal effects of a situation or human action.

Also, three articles in the Spanish Civil Code specifically regulate third-party rights or their protection: Article 1.257 establishes that when the parties agree rights in favour of a third party, this third party will be entitled to enforce these rights unless the obligation is previously revoked; Article 1.259 establishes that any agreement agreed on behalf of a third party can be enforced by the third party unless the counterparty previously revokes it; and Article 1.902 guarantees that anybody to whom a damage is caused has the right to be indemnified. According to the civil law approach, third parties are always passive subjects or entities that can be affected by the activity of others.

Article 2 (f) of the Directive establishes the meaning of this concept in a similar way to the civil law and the Article 29 Working Party affirms that both meanings are the same.

But the Article 29 Working Party also recognizes that the Directive establishes prohibitions, limitations and obligations for third parties that process data.

These rules in the Directive are outside the limited scope of the provisions in civil law and by regulating how third parties must carry out their data processing activities, the Directive does not restrict the scope of this concept to that passive role of third parties in civil law. Under the Directive, third parties process data and

---

4 The term “third party” shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.

5 Article 1.257 of the Spanish Civil Code 1.889: ‘Contracts will only be effective between the parties that execute them and their heirs. … If the contract contains any stipulation in favour of a third party, the latter may enforce its performance provided that it has made its acceptance known to the obligor before it is revoked.’

6 Article 1.259 of the Spanish Civil Code 1.889: ‘Any contract entered into on a person’s behalf without that person’s authorization or empowerment will be null, unless it was ratified by the represented person before the other contracting party revoked it.’

7 Article 1.902 of the Spanish Civil Code, 1.889: ‘Anybody who, as a result of an action or an omission, damages another party through his or her fault or negligence will be obliged to repair any damage caused.’

8 Article 29 Working Party, ‘Opinion 1/2010 on the concepts of “data controller” and “data processor”’ (WP 169, 16 February 2010), 31: ‘The Directive uses “third party” in a way which is not dissimilar to the way in which this concept is normally used in civil law, where [the] third party is usually a subject which is not part of an entity or of an agreement. In the data protection context, this concept should be interpreted as referring to any subject who has no specific legitimacy or authorization—which could stem, for example, from its role as controller, processor, or their employee—in processing personal data.’

9 Article 29 Working Party, ‘Opinion 1/2010 on the concepts of “data controller” and “data processor”’ (WP 169, 16 February 2010), 31: ‘The Directive uses this concept in many provisions, usually with a view to establish prohibitions, limitations and obligations for the cases where personal data might be processed by other parties which in origin were not supposed to process certain personal data.’
must follow some prohibitions, obligations, and limits and consequently the role of these third parties is active even though the definition of Article 2 (f) does not establish it.

Thus, Article 7 (f)\textsuperscript{10} of the Directive uses the concept of ‘third parties to whom data are disclosed’ that is more limited than the concept of Article 2 (f). Third parties to whom data are disclosed (i) are other than the data subject, the controller, the processor, or those who process the data under the controller's or the processor's authority, and (ii) carry out their own data processing, thus fulfilling their own interests, without determining their purposes and means. The phrase ‘third parties to whom the data are disclosed’ in Article 7 (f) refers to a qualified third party and grants it its seal of approval.

Moreover, Articles 11, 12, and 14 of the Directive set out several applicable provisions that place this role opposite to the controllers’ role.

First, Article 7 (f) expressly recognizes the possible existence of entities or individuals different from the data controller that process personal data (it is obvious that the phrase ‘third parties to whom the data are disclosed’ does not refer to the data controller, since both concepts are contrasted in this provision). Interpreting that the role of the third party is an interim situation, at the end of which this party will become data controller or data processor depending on the circumstances, is not admissible because the contrast arising between the terms ‘data controller’ and ‘third party’ makes this impossible and, moreover, the definition itself of data controller given in Article 2 (d) also prevents undefined situations from arising temporarily.

Second, under Article 7 (f), third parties to whom the data are disclosed do not qualify as data processors, as this article expressly sets out that these ‘third parties’ pursue a legitimate interest by processing the data, preventing this processing from being qualified as having been carried out on behalf of the data controller. Moreover, there is no reason why the Directive would not use the name it establishes and attributes to data processors.

Third, by establishing that, in these cases, Member State law must guarantee the legitimacy of personal data processing, the Directive gives prevalent importance to the self-interested pursuit of ‘third parties’, which is only conditioned by the need to achieve a balance between the interest pursued and the interests of the party concerned.

Ultimately, this provision defines and legitimizes the role of the third party to whom personal data are disclosed, comparing it to the roles of the data controller and the data processor. Under Article 7 (f), the third parties to whom the data are disclosed

\textsuperscript{10} ‘Member States shall provide that personal data may be processed only if: … (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1) [of the Directive]’
are entitled to process personal data to satisfy a legitimate, unique, and personal interest, however, they must adapt data processing to the purposes and means determined by another entity that controls that process.

**Key distinguishing features from data controllers and data processors**

To distinguish between the data controller, the data processor, and the third party to whom data are disclosed, it is necessary to ascertain whether those performing the data processing actually decide on the purposes and means of the processing, or have a personal interest in the process.

**Data controllers**

Determining the means of data processing involves making a decision on how personal data are processed, that is, which physical and logical means are used to achieve the purpose sought through data processing. The entity that establishes the processing means takes on the role of the data controller by making this decision.

According to the concept given in the Directive, it is not necessary that the processing means are particular to the data controller. If an entity is entitled to decide whether personal data will be processed by a particular computer system, and orders or allows this system to process personal data, by making this decision it assumes the role of the data controller of the processing.

Moreover, determining the processing means must also be understood to include a passive element, entailing permission by omission, and even unintentional permission. If the data controller's duties include (i) preventing third parties from accessing information improperly by implementing the security measures established under Article 17.1 of the Directive, and (ii) even the duty of secrecy implied in this same article in relation to Article 16, the failure to prevent third parties from gaining unauthorized access would be construed as passive determination, by omission, of the processing means.

Therefore, when an entity decides that the personal data must be included in a data processing system, or does not to take the necessary measures to prevent this from happening, this entity assumes the role of data controller.

Moreover, determining the processing means does not prevent the data processor being given some room for manoeuvre when determining the means that will be used for data processing.

The Article 29 Working Party highlights that the differentiating factor, based on determining the means and the purposes of processing, cannot be interpreted restrictively, and thus an entity will not lose its status as data controller if it gives a third entity (the data processor, in the case taken into consideration by the Working
Party) some margin of discretion when determining the purpose, and flexibility when taking decisions. Because of the incidence, significance, and level of liability involved, this discretion should be greater when determining the means than when determining the purposes.\footnote{11}

Focusing on the second factor affecting the concept of data controller, it is possible to affirm that determining the purposes of processing includes the intents for which personal data are applied, and the decision as to why personal data are processed.

The Directive assigns liability for processing to the entity that determines the purposes, simply because this decision is an act of disposition of personal information that can only be implemented by those authorized to dispose of this data. There is no greater responsibility than deciding to which purposes personal data are applied.

As highlighted above, it is much less likely that the data processor will be given any degree of autonomy to decide the purposes of processing than to decide the means of processing, as the former is infinitely more significant.

**Data processors**

Finally, the existence of a legitimate interest that is intended to be achieved through data processing attributable to both data controllers and third parties to whom the data are disclosed according to Article 7 (f) of the Directive can be considered the key element distinguishing between the third parties to whom the data are disclosed and data processors.

Anyone who physically carries out data processing under the control of a different entity that determines its means and purposes to fulfil a legitimate personal interest will act as a third party to whom data are disclosed, within the meaning set out in Article 7 (f) of the Directive; but when the data processing is carried out for someone else’s interest, they will act as a data processor because, in this case, they will act on behalf of the entity that holds the interest in processing the data.

The interest that is intended to be fulfilled through data processing should not be confused with the purpose of the data processing. Although the purpose and interest may coincide, this is by no means necessary or invariable. Even though the...
meaning in dictionaries of both terms is very close, the reality is that the use of each of these terms in the Directive is always consistent and clearly different.

The purpose of data processing refers to the objective or material result pursued through processing the personal data it focuses on, the information or the conclusion targeted as a result of processing the data of interest, or in the inferences made based on the personal data that are being processed. In this sense, the Directive refers to the purposes of the data processing when regulating the information obligation in Articles 10 (c) and 11 (b), not obliging the data controller to inform about its interest in the data processing, and also makes several references to the purpose of different kinds of data processing in recitals (28), (30), and (37), and Article 4.1 (c). In contrast, the interests that are intended to be fulfilled through the data processing reveal an entirely subjective aspect, namely the project, business, or activity being developed and for which data processing is essential. The interests pursued by data processing are based on an intention, and are a completely volitional and abstract element for which data processing operations can be used as a necessary tool.

The Directive never refers to the ‘interest of the processing’ but to the ‘interest of’ an entity or individual, referring always to a subjective intention in recitals 30, 42, 45, and Articles 7 (f), 8 (b), 13.1 (e), and 26.1 (c) and (e).

Consequently, article 7 (f) of the Directive grants its seal of approval to a different assumption concerning the data controller and the data processor, applicable to anyone who carries out data processing as an essentially personal activity, to develop a project or interest ascribed only to them, while limiting data processing to the means and purposes determined by a different party that, therefore, will be liable for this data processing, the data controller.

**Legal status of third parties to whom personal data are disclosed**

As mentioned above, the Directive contains several special provisions that apply to these third parties to whom the data are disclosed. Further to regulating its legitimacy these special provisions affect the duty of information and the duty to attend to the rights of rectification, cancellation, and opposition, and give rise to a unique legal regime.

**Legitimacy**

In accordance with Article 7 (f) of the Directive, the third party to whom the data are disclosed is only entitled to process data if the interest or the rights and freedom of the data subject do not prevail over the legitimate interest pursued. This limitation encourages the third party to whom the data are disclosed to assess the impact caused by the data processing carried out over the interests and fundamental rights of the data subject, which appears to be a precedent for the
‘data protection impact assessment’ regulated in Article 33 of the Proposal for a General Regulation on Data Protection\textsuperscript{12}, which is currently being processed.

Analysing this impact implies comparing the interest pursued with the consequences this would have on the data subject. Article 7 (f) of the Directive disallows data processing in cases where the desired result does not justify the means that are used, that is, when any limitation to interests, fundamental rights, or public freedom is not justified by the significance and importance of the interest pursued through the data processing.

It is worth noting that Article 7 (f) of the Directive requires that not only the rights and fundamental freedom are taken into consideration, but also the (common) interests of the individual concerned.

Any reference to common interest should be limited to the interest which can commonly and generally be attributed to individuals at any particular moment, and under conditions and social customs that concur objectively or generally; but not extended to the exclusively personal and subjective interests of each data subject (the mere preferences), since including personal preferences in the analysis of the impact on data protection would require an individualized enquiry that would make them known, that is, an authorization for consent. However, the authorization for consent is regulated in Article 7 (a)\textsuperscript{13} of the Directive, and their inclusion in the impact analysis, set out in paragraph (f), would invalidate this provision.

**Obligation to inform**

Second, the third party to whom the data are disclosed has no obligation to inform the data subjects about data processing. Under the Directive, this is the data controller’s obligation.

Article 11 (1)\textsuperscript{14} of the Directive makes explicit reference to the third parties to whom the data are intended to be disclosed, so there is no doubt that the controller is the only recipient of this obligation and the third party is excluded from it.


\textsuperscript{13} ‘Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent’

\textsuperscript{14} '1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

\begin{enumerate}
\item the identity of the controller and of his representative, if any;
\item the purposes of the processing;
\item any further information such as
\begin{itemize}
\item the categories of data concerned,
\item the recipients or categories of recipients,
\item the existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.
\end{itemize}
\end{enumerate}
Before providing the data to a third party, the data controller must inform the data subject, and the information provided will guarantee that the data processing carried out by the third party to achieve its own interests does not infringe on the data subject's interests and rights since, as highlighted subsequently, the data subject can object to this disclosure.

**Rights of rectification and cancellation**

Third, the Directive requires that controllers deal directly with any applications for the rectification or cancellation of data requested by data subjects. Third parties to whom the data are disclosed are not required to deal with any applications from data subjects, and are only obliged to fulfil the data subjects' requests when the controller reports them.

Article 12 (c)\(^{15}\) of the Directive also contrasts the concept ‘controller’ with that of ‘third party to whom the data are disclosed’, which leads to the affirmation that this provision consciously excludes third parties from the obligation imposed only on controllers. Thus, the Directive ensures data subjects that the third party to whom the data are disclosed will comply with the principles of data quality as provided in paragraphs (c) and (d) of Article 6 of the Directive, since the data will be adapted to this principle of quality as soon as the controller notifies the third party of the need to rectify, erase, or block this data.

**Right of opposition**

Furthermore, as regards the right of opposition, Article 14 (a)\(^{16}\) of the Directive establishes that it is a right to ask the data controller to cease processing the data, and to instruct the third party to stop processing. However, the Directive does not guarantee that those affected will have the right to demand that the third party must cease processing data, but to ask the data controller to notify the third party of this.

Despite the vagueness of Article 14 (a), the end prohibition on the data controller to continue processing data is evidence of the fact that the opposition provided for in this first section can only be exercised against the controller. In this case, the third party must stop processing as soon as the notification provided for in Article 12 (c) of the Directive is received.

---

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

\(^{15}\) Member States shall guarantee every data subject the right to obtain from the controller: … notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

\(^{16}\) ‘Member States shall grant the data subject the right: (a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;’
The second assumption regulated in Article 14 (b)\textsuperscript{17} has a very limited scope. It only regulates data disclosures to third parties for the purpose of direct marketing, and, again, this is only applicable to data controllers, since its wording establishes the right to receive a notification that can only be required of the controller before disclosing any data to the third party or, subsequently, when the third party intends to use this data for advertising, so an objection to the process can only be made to the controller.

From this set of provisions, it is possible to affirm that the Directive contains a special regime for data processing applied in cases in which processing is carried out under a concept that differs from those of data controller and data processor. The Directive describes ‘third parties to whom the data are disclosed’ as entities that carry out this unique processing.

In these cases, data protection of data subjects is guaranteed through prior information regarding the disclosure of data to third parties, which is the duty of the controller, and through the controller's obligation to forward the opposition and information updating applications to third parties to whom the data have been disclosed. Consequently, the ‘third parties to whom the data are disclosed’ are able to carry out data processing without having to deal directly with these obligations towards data subjects.

Obviously, to apply this regime, ‘third parties to whom the data are disclosed’ cannot determine either the purposes or the means of data processing; otherwise they would be controllers of the processing, which would prevent the special provisions from being applied. If those processing data do not have at least a proper and legitimate purpose, but do so on behalf of the controller, they would not have the status of ‘third party’ but of data processor, with the applicable special regime.

**Processing assumptions regarding third parties to whom the data are disclosed**

Finally, reference is made to some data processing assumptions that have raised complex discussions on the role of the entity that processes data and whose cause lies in the fact that the entity carrying out data processing clearly does not fall within the concept of data controller (does not determine the purposes and means of processing) and undoubtedly, they cannot be considered data processors because they do not perform the process on behalf of the controller. All these cases fit the Directive's concept of ‘third party to whom the data are disclosed’.

---

\textsuperscript{17} ‘Member States shall grant the data subject the right: … (b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).’
Telecommunications or electronic mail service

Telecommunications companies are probably those who manage the greatest volume of information to conduct their business, but they do not have to be bound to the controller by any service agreement, or even know who the controller is. They merely provide a connectivity service to ensure that the message gets through their systems to the recipient.

These companies conduct their business by intermediating in the flow of communications but they process the information in the messages that they manage without determining the means and purposes, which are fixed by the person who originates the message, they only make their own telecommunications systems available to their clients (who may be the recipients of messages, or even other companies that also mediate in the telecommunication service).

Clearly, telecommunications companies have a direct interest in the data processing they carry out and for this reason they have created a data processing scheme for their own economic benefit, but they do not make decisions regarding data processing. This is reflected in Recital 47\textsuperscript{18} of the Directive, which excludes telecommunications companies from the concept of data controllers, except for personal data additional to the message that they need to operate their service. The Directive on privacy and electronic communications\textsuperscript{19} regulates their role as controllers of this data.

As they are excluded from the Directive's concept of controller, and they cannot be classified as data processors, it is implied that the Directive considers that these companies process personal data according to a different concept of controller and processor. In this case, the legal regime regarding third parties to whom the data are disclosed, established by the Directive, is entirely applicable.

Advocate General Jääskinen also took into consideration Recital 47 of the Directive when analysing the role of search engines as mere intermediaries and concludes that search engines are not proper data controllers\textsuperscript{20}.

Credit bureaus

\textsuperscript{18} Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service.


\textsuperscript{20} Opinion of AG Jääskinen delivered on 25 June 2013 ECJ Case C 131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González § 36: 'The European Union has attached great importance to the development of the information society. In this context, the role of information society intermediaries has also been addressed. Such intermediaries act as bridge builders between content providers and internet users. The specific role of intermediaries has been recognised, for example, in the Directive (recital 47 in the preamble thereto), in the ecommerce Directive 2000/31 (24) (Article 21(2) and recital 18 in the preamble thereto) as well as in Opinion 1/2008 of the Article 29 Working Party. The role of internet service providers has been considered as crucial for the information society, and their liability for the third-party content they transfer and/or store has been limited in order to facilitate their legitimate activities.'
Credit information data files on solvency, known as credit bureaus, should also be referred to. In this case, credit bureau companies create a data processing scheme for their own economic benefit, but make no decisions regarding data processing. Creditors are people who, due to loan defaults, decide to upload the debtors' personal data so that other entities can access them easily and be aware of this situation before granting a new loan.

If the credit bureaus are limited to processing information on the basis of the purposes and means specified by the controller, the role of these companies clearly falls within the definition given to third parties to whom data are disclosed. Obviously, if the company operating the credit bureau processes the reported data for any purpose other than the purpose determined by the creditor, or applies any processing means other than those set out by the creditor (by adding to the recorded information using data from other sources, not updating or making information accessible to third parties after receiving instructions to block this information, for example), this company would then become the controller, as it determines the purposes and means of processing.

In the case of Spain (which is my country), these data files are specifically regulated by the Organic Law on Protection of Personal Data21 (LOPD), which establishes a specific regime in Article 2922 that has developed the Regulation implementing this Organic Law23 (RPD), and conforms to the regulations established under the Directive.

The credit bureau does not have the consent of the data subjects; rather, the creditors have the legal capacity to process data. The creditor (data controller) processes the debtor's data to execute the credit agreement. In this regard, Article 3924 of the RPD requires the contract terms and conditions to establish that in the event of default, the debt will be recorded in the bureau, thus comprising processing in compliance with Article 7 (b)25 of the Directive.

22 '1. Providers of information services on creditworthiness and credit may process only personal data obtained from registers and sources accessible to the public and set up for that purpose or based on information provided by the data subject or with his consent.
2. Processing is also allowed of personal data relating to the fulfillment or non-fulfillment of financial obligations provided by the creditor or by someone acting on his behalf. In such cases the data subjects shall be informed, within a period of thirty days from the recording, of those who have recorded personal data in files, with a reference to the data included, and they shall be informed of their right to request information on all of them under the conditions laid down by this Law.
3. In the cases referred to in the two paragraphs above, and at the request of the data subject, the data controller shall communicate to him the data, together with any assessments and appreciations made about him during the previous six months and the name and address of the person or body to whom the data have been disclosed.
4. Only those personal data may be recorded and transferred which are necessary for assessing the economic capacity of the data subjects and which, in the case adverse data, do not go back for more than six years, always provided that they give a true picture of the current situation of the data subjects.'
24 'The creditor shall inform the debtor, upon the formalization of the contract and, in any case, upon making the request to which letter c) of subsection 1 of the previous article refers, that should payment not be made under the terms provided for this purpose and the requirements provided in the aforesaid article be fulfilled, the data relating to the non-payment shall be disclosed to files relating to the fulfilment or non-fulfilment of pecuniary obligations.'
25 ‘Member States shall provide that personal data may be processed only if: ... (b) 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;’
The creditor informs the bureau, laying claim to a legitimate interest, such as obtaining payment of an overdue loan (Article 7 (f) of the Directive), and seeking the fulfilment of a contractual obligation (Article 7 (b) of the Directive), which justifies that processing would not be affected by the debtor's opposition.

The credit bureau processes data in accordance with the purpose (communication to third parties) and the means (the computer system used by the credit bureau) that the creditor has determined, to achieve its personal interest (to achieve the aim of its business, which is precisely to carry out this data processing), as established in Article 7 (f) of the Directive.

The data controller, that is, the creditor, must report on the possible inclusion of the data in a file when requesting payment from the debtor (Article 11 (1) of the Directive); likewise, the creditor must keep the information updated in the bureau (Article 12 (c) of the Directive).

As mentioned above, the debtor's right to object to the controller recording the data in the bureau (Article 14 (1) of the Directive) does not apply in this case, as it is needed to execute the contract (Article 7 (b) of the Directive), as established under article 39 RPD, and authorized under Article 14 (1) of the Directive itself.

The RPD establishes some rules that do not reflect the regime established by the Directive, including the bureau's obligation to (i) notify the debtor that debts are recorded (Article 40.126), and (ii) receive and channel applications to access, update, and cancel data (Article 4427). However, as this is a case of data processing to which the debtor cannot object, these additional guarantees cannot be considered an exception or violation of the Directive's principles, but compensation for the exception of the right to object.

Credit bureau data processing has caused an ongoing controversy because credit bureaus do not seem to perfectly fit the concept of data controller. Even the

---

26 'The data controller of the joint file shall notify the data subjects for whom personal data has been registered, within thirty days from such registration, a reference of those data that have been included, thus informing them of the possibility to exercise their rights of access, rectification, erasure and objection, under the terms established in Organic Law 15/1999, of 13 December.'

27 '1. The exercise of the rights of access, rectification, erasure and objection is subject to the provisions of Chapters I to IV of Title III hereof, without prejudice to the provisions contained in this Article.

2. When the data subject exercises his right of access in relation to the inclusion of his data in a file regulated by Article 29.2 of Organic Law 15/1999, of 13 December, the following rules shall be borne in mind:

1°. If the request is addressed to the owner of the joint file, he shall communicate to the data subject all the data relating to him recorded in the file. In this case, the owner of the joint file shall, as well as fulfilling the provisions hereof, provide the evaluations and assessments regarding the data subject that have been disclosed in the last six months and the name and address of the recipients.

2°. If the request is addressed to any other participant in the system, he shall communicate to the data subject all the data relating to him to which they have access, as well as the identity and address of the owner of the joint file so that the data subject may complete his right of access.

3. When the data subject exercises his rights of rectification or erasure in relation to the inclusion of his data in a file regulated by Article 29.2 of Organic Law 15/1999, of 13 December, the following rules shall be borne in mind:

1°. If the request is addressed to the owner of the joint file, he shall take the relevant measures to transfer the request to the entity that has provided the data, so that it may answer the request. If the data controller for the joint file has not received an answer from the entity within seven days, he shall proceed with the precautionary rectification or erasure of the data.

2°. If the request is addressed to the provider of the data to the joint file he shall proceed with the rectification or erasure of the data in his files and shall notify the owner of the joint file within ten days, also answering the data subject under the terms provided in Article 33 hereof.

3°. If the request is addressed to another participant in the system, who has not provided data to the joint file, this entity shall inform the data subject of this fact within ten days, also providing the identity and address of the owner of the joint file so that, if necessary, the data subject may exercise his rights before him.'
Spanish Data Protection Authority (the Agency) and the RPD refer to them as ‘joint files’, highlighting the fact that creditors make the decision on the means and purposes of the data that are recorded. The Agency itself coined the term ‘file controller’ to distinguish a bureau from a data controller, because of differences arising in each of these cases. Also, the Supreme Court of Spain has declared in two rulings that only bureaus can be held liable for infringements, and not the creditors that write down the default credit, because under the LOPD liability can only be attributed to file controllers, and not to those who provide the bureau that information fulfilling an agreement executed with them. Nevertheless, the Spanish courts have now changed their approach and do not exclude from liability creditors that fail to fulfil the legal guaranties when recording default debts.

All these circumstances highlight that this kind of data processing is singular. This singularity derives from the fact that those carrying out the processing do not act as a controller or as a processor, but as a third figure, namely a third party to whom the data are disclosed, as regulated under the Directive, that understandably cannot be given the same liability as the data controller, as long as it does not assume the role of data controller to determine its means and purposes.

**List brokers**

Another case of data processing that falls within the concept of ‘third parties to whom the data are disclosed’ is carried out by companies known as ‘list brokers’, which receive lists from other companies that have obtained personal data through their commercial traffic (including customers and prospective customers). List brokers deal with those lists in their own name through advertising, seeking advertisers who are interested in sending out publicity.

The list broker carries out data processing for its own interest, given that it can benefit economically from this data, an interest considered legitimate and in accordance with the principles established in Article 7 (f) of the Directive.

The list provider, on the other hand, decides which data the list broker will use, and for what purpose and by which means, as it is the list provider who decides that the list will be used by the list broker for direct marketing, making the list provider a...
company that falls within the concept of controller as defined in Article 2 (d) of the Directive. It is required to update the list, respecting the data subjects' right of objection and cancellation, and must ensure quality data, under Article 6 (c) and (d) of the Directive.

In this case, the list broker does not seem to perfectly fit the concept of data processor, as it has a direct interest in the processing it carries out from the moment when it obtains the results deriving from using the list developed, which makes it impossible to interpret whether it acts on behalf of the controller. It cannot be considered as a data controller, because the purposes and means of processing are determined by the company that provides its data for commercial use. This is another ‘third party to whom the data are disclosed’ that processes those data for its own personal interest, always according to the purposes and means determined by the supplier of the list that fits to the role of data controller.

Of course, in cases where the list broker can decide on the purposes and means of the processing of the data (a common occurrence), the list broker must not be described as a third party, but as a data controller.

Moreover, it should also be emphasized that Article 14 (b)\(^\text{29}\) of the Directive provides an additional guarantee for this kind of data processing, greatly strengthening the balance between the competing interests of the data subject and the third party to whom the data are disclosed for advertising, because it forces the controller to provide enough information to the data subject for it to object at an early stage to allowing the data to be subject to this disclosure or use, or later, if the controller authorizes the third party to use the list for marketing purposes at a later date.

This case of data processing has also been analysed by the Agency, which, as in the previous case, has distinguished the role of list broker by calling it a ‘file controller’. It is logical that the liability for the processing of the data should fall on the supplier of the list, who must keep it updated by deleting and amending it as necessary, and, unless the list broker carries out data processing in a way that differs from the supplier's specifications, it makes perfect sense to exonerate the list broker of any liability.

**Internet search engines**

Internet search engines should also be included in these considerations. Search engines download the content any user decides to publish on the internet (the content ‘editor’) in the same way other users would, but massively and systematically, using programmed browsers known as ‘robots’. ‘Robots’ are computer programs that control the search engines to download content.

---

\(^{29}\) Quoted in n 17.
Search engines follow a working protocol under which web editors include instructions on their websites for the search engines, permitting them to download and index the published contents (‘robot.txt’ protocol). Through these instructions, search engines are authorized or not to use content published for the provision of their service; some instructions may also be aimed at a particular search engine.

This protocol is available to editors and its use is widespread because it is simple and rarely causes any incidents. This means that editors have the power not only to decide to publish certain content and keep it published, but also to authorize or condition whether web users can locate the content using the search service. Editors are data controllers, as the Article 29 Working Party and the AG Jääskinen have declared. Nevertheless, the ECJ has declared that this protocol does not reduce the control and responsibility of search engines.

After downloading the files, the search engines copy them into their own systems and process them to extract and classify the words contained in the texts and downloaded hyperlinks, creating a list (index) that links each word with the website where it was found. The index allows search engines to deal with the search requests by identifying in the index the words that the user enters as a search query and, depending on the degree of coincidence with the search query and other criteria, to offer a list of search results.

When proper names of people are included in the index, there is a data processing function which enables search engine users to find published information on the Internet relating to that person.

As long as search engines limit their service to being an intermediary in the search for content, the Article 29 Working Party and Advocate General Jääskinen affirm

---

31 ECJ: Case C 131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González: Judgment of the Court (Grand Chamber) 13 May 2014: 39 Finally, the fact that publishers of websites have the option of indicating to operators of search engines, by means in particular of exclusion protocols such as ‘robot.txt’ or codes such as ‘noindex’ or ‘noarchive’, that they wish specific information published on their site to be wholly or partially excluded from the search engines’ automatic indexes does not mean that, if publishers of websites do not so indicate, the operator of a search engine is released from its responsibility for the processing of personal data that it carries out in the context of the engine’s activity.’
32 Article 29 Working Party, ‘Opinion 1/2008 on data protection issues related to search engines’ WP 148, 4 April 2008, 14: ‘The principle of proportionality requires that to the extent that a search engine provider acts purely as an intermediary, it should not be considered to be the principal controller with regard to the content related processing of personal data that is taking place. In this case the principal controllers of personal data are the information providers. The formal, legal and practical control the search engine has over the personal data involved is usually limited to the possibility of removing data from its servers. With regard to the removal of personal data from their index and search results, search engines have sufficient control to consider them as controllers (either alone or jointly with others) in those cases, but the extent to which an obligation to remove or block personal data exists, may depend on the general tort law and liability regulations of the particular Member State.’
33 Opinion of AG Jääskinen delivered on 25 June 2013 Case C 131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González: ‘88. The Article 29 Working Party has emphasised that, first and foremost, the purpose of the concept of controller is to determine who is to be responsible for compliance with data protection rules and to allocate this responsibility to the locus of the factual influence. [Article 29 Working Party, Opinion 1/2008, pp. 4 and 9.] According to the Working Party, ‘[t]he principle of proportionality requires that to the extent that a search engine provider acts purely as an intermediary, it should not be considered as the principal controller with regard to the content related processing of personal data that is taking place. In this case the principal controllers of personal data are the information providers.’ [Article 29 Working Party, Opinion 1/2010, 14.]
In my view the internet search engine service provider cannot in law or in fact fulfil the obligations of controller provided in Articles 6, 7 and 8 of the Directive in relation to the personal data on source web pages hosted on third-party servers. Therefore a reasonable interpretation of the Directive
that search engines do not fit the role of data controller and that this data controller role clearly corresponds to the website editor.

Nevertheless, opposite to the opinion of article 29 Working Party and Advocate General Jääskinen, the ECJ has declared recently that search engines are data controllers when they index personal data published on websites.

Although, under the interpretation defended in this article, the data processing carried out by the search engines falls within the concept of a ‘third party to whom the data are disclosed’ because the search engine, without prejudice to having developed the infrastructure to provide the service, follows the instructions determined by web editors (robot.txt protocol or codes ‘noindex’ or ‘noarchive’). In this case, editors also determine the means and purposes of processing the data indexed and, therefore, act as data controllers for this processing, while search engines process the data according to the editor’s specifications, yet on their own behalf, carrying out a separate activity.

And, again, it makes perfect sense that the publishers should be responsible for reporting the disclosure of data to search engines, for channelling the cancellation and update requests (using robot.txt protocol or codes ‘noindex’ or ‘noarchive’), and for promptly updating the content for the search engine to refresh the information, accurately reflecting the content published.

This is particularly relevant when the provisions of the Directive are applied to the search engines regarding the third party to whom the data are disclosed: under the interpretation defended here, the ‘editors’ (who publish the contents), if applicable, must inform the data subjects of their intention to publish content on the Internet, facilitating its location through search engines. The editors are also obliged (on the basis of the robot.txt protocol) to prevent this, if data subjects object to it or request that this information cannot be found through a search engine when their name is introduced.

And of course, if the search engine determines the means or purposes of processing, it will lose its role as a third party to whom the data are disclosed and

34 ECJ: Case C 131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González: Judgment of the Court (Grand Chamber) 13 May 2014: ‘1. Article 2(b) and (d) of 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 are to be interpreted as meaning that, first, the activity of a search engine consisting in finding information published or placed on the Internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as ‘processing of personal data’ within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the ‘controller’ in respect of that processing, within the meaning of Article 2(d).’

35 It should be borne in mind that, in the case of publications, the author frequently exercises freedom of information and expression, which, in practice, leads to the author not informing the subjects referred to in the content of their intention to make public the information it publishes.
become a controller. This will occur when the search engine provides added-value services, or when retaining the indexed data on a long-term basis after its access has been blocked on the source web browser, or after the content has been modified, as the Article 29 Working Party highlights.

Conclusion

The Directive regulates an assumption beyond the definitions of controller and processor, granting its seal of approval by recognizing its legitimacy, and establishing legal status. Moreover, it is easy to recognize cases that fall within the concept of the third party to whom the data are disclosed. Furthermore, in all of these cases, this concept of the third party to whom the data are disclosed resolves legal questions and problems that arise when trying to subject these ‘third parties’ to the legal regime applicable to controllers and processors.

However, these provisions of the Directive have not been transposed into Spanish law, and I am not aware of any precedent that has argued or proposed that Article 7 (f) of the Directive should be applied in the sense described in this text. Furthermore, the ECJ has ruled out Case C 131-12, affirming clearly that search engines are data controllers when they index personal data published on websites, impeding the interpretation defended here.

Although the proposal of the Regulation of the European Parliament and of the Council, ‘on the protection of individuals with regard to processing of personal data and on the free movement of such data’, removed from Article 6 all references to the third parties to whom the data are disclosed, it has been reintroduced in the text voted by the LIBE committee last October and the European Parliament confirmed this in the Position adopted at the first reading on 12 March 2014.

From my point of view, although nobody has ever defended it, this interpretation helps to differentiate the data controller from those to whom the data controller discloses data to process those data under licence and the data controller’s instructions, but do not act as data processors.

The obligations and liability of these third parties to whom data are disclosed should be different while following the data controller’s instructions and conditions,

---
36 Article 29 Working Party, ‘Opinion on data protection issues related to search engines’ WP 148, 4 April 2008, 24: ‘In their second role, as providers of content data (such as the data in the index), generally they are not to be held as primarily responsible under European data protection law for the personal data they process. Exceptions are the availability of a long-term “cache” and value added operations on personal data (such as search engines aimed at building profiles of natural persons). When providing such services, search engines are to be held fully responsible under the Data Protection Directive and must comply with all relevant provisions’.

37 Article 6 ‘Lawfulness of processing’ of the text of the proposal for a regulation of the European Parliament and of the Council, ‘on the protection of individuals with regard to the processing of personal data and on the free movement of such data’ (General Data Protection Regulation) approved by the European Parliament legislative resolution of 12 March 2014 (Ordinary legislative procedure: first reading), Amendment 100: ‘1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: … (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or, in case of disclosure, by the third party to whom the data is disclosed, and which meet the reasonable expectations of the data subject based on his or her relationship with the controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. This shall not apply to processing carried out by public authorities in the performance of their tasks. <www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN>.'
because these parties trust the data controller to grant them the licence to process the data, and they have no power of decision regarding the purposes and means of the data processing.

In addition, the legal status of these third parties is logical and complete, requiring them to follow the data controller's instructions, and they do not reduce the legal rights of data subjects.

For this reason, I defend that the forthcoming General Regulation on Data Protection should regulate expressly the role of these ‘third parties to whom data are disclosed’, regulating their legal status with derogations similar to those established in the Directive.

The new regulation should impose on the data controllers that disclose data to third parties determining the purposes and means of data processing the duty to inform the data subjects about this data processing and keep the data disclosed up to date.

With this legal status, these third parties would be able to develop their activity. Also, the interests of the data subject, the industry and society would be balanced and the right to privacy protected.