

May 2010

Technology

Important new guidance on the concept of "Controller" and "Processor" from The Article 29 Data Protection Working Party

(00264/10/En Wp 169 Adopted February 2010)

Data processing is not what it once was. Solutions have become more sophisticated and are provided through a myriad of different arrangements: hosting solutions, sharing solutions, the engagement of multiple providers in one project or service, chains of providers and complex sub-processing agreements are all increasingly common.

Not surprisingly it is sometimes a challenge to work out how the data protection regime applies in this changed environment. A common example would be where parties "pool" data and then carry out searches of the pooled data and retain records of the searches. Depending on the actors and the arrangements the custodian of the pooled dataset may be regarded as a data processor or a controller in its own right; the parties who access the data may be regarded as controllers acting jointly or as controllers acting separately. Where sophisticated uses and arrangements exist it can be an issue of dispute between parties and agreement must be reached on the roles of the parties. The question of when a party is a mere processor as apposed to a controller has become a difficult one to apply and there has been at least one controversial and high-profile decision over the issue in the SWIFT case.

The identity of the controller is crucial in determining who has to meet the obligations under the law. Where the processing has a cross-border element it will also be crucial in determining which EU law, if any, applies to the processing. Not unexpectedly there have been divergent approaches and the new guidance is welcome.

The Opinion explores and advises on the knotty problems of identifying controllers and processors.

In this piece we explain the approach taken by the Working Party, analyse the Opinion and draw out some practical steps for data controllers to follow in the future.

Article 29 Working Party

For those who are not familiar with the Article 29 Working Party it is composed of senior staff from the data protection regulators in the EU. It was established under Directive 95/46/EC to provide advice, primarily to the European Commission, on the implementation of the Directive and associated matters. It has increasingly offered advice on a wide range of topics and, although its views are not binding, they can be influential, for example in the UK the Information Commissioner's guidance on the term "personal data" was strongly influenced by the Article 29 paper on the same topic.

The Working Party states that it issued Opinion 1/2010 because it noted that "there are signs that there may be a lack of clarity, at least to certain aspects of [the concepts of controller and processor] and some divergent views among practitioners in different Member States that may lead to different interpretations of the same principles and definitions introduced for the purpose of harmonisation at European level."

The Opinion considers the definitions of the terms in the Directive and provides a range of case studies and worked examples, in all 24 examples are given. The examples are necessarily partial and cannot cover every case but they offer a good spread of different models and provide a helpful reference point.

Overview

The Opinion is over 30 pages long and can be rather repetitious but it has a useful Executive Summary which makes the following main points:

- The concept of a controller should be interpreted according to Community not national law;
- The decision to attribute responsibility as a controller will be based on the facts of each case rather than being purely a technical legal issue;
- The three elements of the definition of a controller in the Directive are important, those are that there must be an identifiable legal entity, the controller must determine purpose and means of processing; and control may be "pluralistic" that is carried out alone or jointly;
- The controller can delegate all or parts of his processing to a processor;
- The distinction between controllers and processors remains valid and workable.

Relevant definitions

The Directive defines a data controller as " 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".

A data processor "shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller".

The national law applicable to the processing of personal data is determined by the place of establishment of the data controller. Article 4.1(a) provides that, the Directive must be applied by Member States where; "the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable."

Section 5 of the UK Data Protection Act 1998 includes mirror provisions to Article 4.1(a). It provides that the Act applies to a data controller in respect of personal data if the data controller is established in the UK and the personal data are processed in the context of that establishment. A person is treated as being established in the UK if it (among other tests) is a body incorporated under the law of the UK.

Role of the controller

The Opinion re-states that the purpose of the Directive is the protection of the personal data of individuals; it is important to determine who is the data controller for the purposes of allocating responsibility for meeting the data protection rules and ensuring that data subjects can exercise their rights. It is also important in establishing which national law applies to the processing in question particularly in the light of the key challenges which have arisen from the changes in technology, increased globalisation of services and organisational developments.

The substantive obligations to meet data protection standards rest with the controllers, not processors (although processors may have some limited security obligation). The identity of the controller is therefore critical to ensure that those standards are delivered.

The Opinion refers to the SWIFT decision in which it was held that SWIFT, which was processing financial data on behalf of banks, was a data controller despite the fact that the contract with the banks classed it as a data processor.

The Opinion states that the decision was based on the fact that SWIFT allowed US authorities to access the database and in doing so exercised a degree of control which was incompatible with the role of a data processor. While this would be a logical reason to hold that SWIFT was a controller we are aware that the decision in SWIFT does not cite the provision of access as the main reason for determining that SWIFT was a controller. The main thrust of the reasoning in the decision itself appeared to be that SWIFT controlled the nature of the processing carried out in the system. This aspect of the reasoning in the decision in SWIFT has been heavily criticised and given rise to concerns among business. It appears from the Opinion (and its re-writing of the reasoning in the decision) that the consensus view of the data protection regulators in the EU, is to move away from that approach. This will be welcomed, especially by providers of sophisticated outsourcing services.

Applying the definitions

The Opinion considers the meaning of the term "determines" the manner and purpose of the processing.

It points out that the power to determine must be exercised by the controller. A party cannot be a controller simply because it is formally designated as such irrespective of the real power. In making a determination someone may be acting unlawfully but the fact that the control is unlawful does not stop the party being a controller. It further states that the concept is autonomous, in other words the creator of a dataset or the holder of intellectual property rights will not necessarily be a controller, although as a matter of fact the controller may be both.

It also states that, outside those areas where a party holds a clear legal responsibility for particular processing, as is the case with public authorities, the question is largely a question of fact. This must be determined by an analysis of all the facts of the case.

It points out that the examples where control is exercised because of the party's legal obligations are relatively straightforward; the more difficult cases arise where the purpose and means of the processing are not determined by law but by agreement between the parties. The bulk of the remainder of analysis is devoted to examples drawn from the private sector.

Assessing the identity of the controller

In considering the position of private parties it states that contractual terms may be important but are not determinative; the example of the SWIFT system is given in this context.

It goes on to tackle the critical question of the level of detail at which control must be exercised stating,

"When it comes to assessing the determination of the purpose and the means with a view to attribute the role of data controller the crucial question is therefore to which level of detail somebody should determine purposes and means in order to be considered as a controller. And in correlation to this, which is the margin of manoeuvre that the Directive allows for a data processor".

It goes on to announce that, "A pragmatic approach is needed, placing greater emphasis on discretion in determining purposes and on the latitude in making decisions."

In doing so it refers to the equivalent definition in Treaty 108, the Council of Europe Convention which pre-dates the Directive, which covered control of purpose, content of data, operations and third party access. It construes the definition in the Directive taking account of that history and therefore focuses on what are described as the essential elements of control being issues such as "Which data shall be processed?" "Who shall have access to data?" rather than just which hardware or software shall be used. It accepts that the "means" of processing can be delegated to processors under general guidance.

This is a familiar theme to anyone who uses the UK Commissioner's Guidance on this point. He takes the view that determination of the purpose of the processing is the "paramount" test of whether a party is a data controller. This statement in the Guidance, although it has always seemed to be a logical and intuitively correct view, was supported by no authority. It is interesting that the Working Party appears to have come to the same position but has managed to find some support for it in the approach of Treaty 108.

Some observations follow about the question of who should be regarded as the "natural person, legal person or other body" to take on the mantle of controller. It expresses a clear view that the controller should be the company or legal person involved in processing and not an individual in an organisation, and distinguishes between the data controller and the data protection officer.

Plurality of control

The rest of the Opinion is taken up with an analysis of how the identity of the controller is decided where there are "multiple actors interacting in the processing of personal data".

The Directive provides for determination of the manner and purpose of processing being made "alone or jointly with others." The Directive includes no concept of control being exercised "in common" as appears in the UK Act. The Opinion therefore sheds no light on what is meant by the term "in common". Clearly it cannot mean something which is outside or different from the concepts set out in the Directive. We would suggest that "in common" should be viewed as a sub-set of joint control.

The Opinion explains the term "jointly", was introduced by the European Parliament during the passage of the Directive and the Commission commented on in its working papers (or travaux préparatoire). The Commission referred to the possibility that "for a single processing operation a number of parties may jointly determine the purposes and means of processing to be carried out" and therefore that in such a case "each of the co-controllers must be considered as being constrained by the obligations imposed by the Directive".

This is the scenario that the Commissioner refers to as "jointly". The UK Commissioner states in the Guidance "Jointly" covers the situation where the determination is exercised by acting together. Determination "in common" is where data users share a pool of information, each processing independently of each other". The existing guidance of the UK Commissioner and the new Opinion would map more clearly onto one another if this mutual type of control was regarded as control "in common" and simply a sub-set of the broader aspect of joint control which can cover, as the Opinion states, a wide range of pluralistic options.

Examples of joint control

The Opinion then goes on to consider cases where "multiple actors interact in the processing of personal data". Much of the rest of the paper is concerned with an analysis of the different models of joint control and worked examples. Some points are straightforward, for example it is clear that any party which makes uses of data for its own purposes will be a data controller for those own purposes.

It makes clear that the mere fact that parties cooperate in processing personal data does not make them joint controllers, "First of all the mere fact that different subjects cooperate in processing personal data, for example in a chain, does not entail that they are joint controllers in all cases, since an exchange of data between two parties without sharing purposes or means in a common set of operations should be considered only as a transfer of data between separate controllers." Where the same personal data is processed by a series of parties in sequence, each using the data for a different purpose then they will remain separate controllers but where they have an element of common purpose they will be joint controllers.

It gives an example of joint control drawn from the travel industry where an agency, hotel and airline cooperate to set up a common platform for a travel reservation system. However, it acknowledges that many systems do not fall neatly on either side of the line drawn here. In many cases the shared systems exhibit an element of cooperation between the parties but are still used to pass information through a chain. The central agency may also supply separate services.

The Opinion goes on to refer to what it calls the "origin-based approach" to allocation of responsibility as a data controller as follows, "Another possible structure is the "origin-based approach" which arises when each controller is responsible for the data it introduces in the system. This is the case of some EU-wide databases, where control, and thus the obligation to act on requests for access and rectification is attributed on the basis of the national origin of personal data."

The next example is of social networking sites. The Opinion states that the sites are the controllers for the platforms as they provide the services which enable individuals to "publish and exchange information" with other users.

The Opinion gives further examples which are relatively clear cut such as the role of an internet service host, which would in principle be a processor for the personal data published on line by its customers, although if the ISP uses the personal data for its own purposes then it would be the data controller for that processing.

The Opinion contemplates the fact that being unable to directly fulfil all of a controller's obligations or having access to the data is not essential as long as the data subjects' rights can be assured by the different participants.

It emphasises that, even in complex data processing arrangements, compliance with data protection should be properly allocated and data subjects should be provided with clear information explaining the various "stages and actors of the processing". Other examples provided cover behavioural advertising and the pooling of default information.

An interesting aspect of the Opinion is the clear acceptance that the concept of joint control under the Directive does not involve "joint and several" legal responsibility for the processing. While there might sometimes be joint and several responsibility this will not be the rule. The Opinion makes clear that where there is plurality of control, each data controller may be responsible, and thus liable for the processing at different stages and to different degrees. However it recommends that joint and several obligations should be considered especially where it is difficult to establish where separate aspects of control begin and end. This reflects its concern that a multiplicity of controllers may lead to fragmentation of proper control and "may also lead to undesired complexities and to a possible lack of clarity in the allocation of responsibilities".

Data processors

The last part of the Opinion is concerned with the definition of "processor". A processor must be a separate legal entity from the controller and must carry out the processing of personal data on behalf of the controller. It accepts that a controller may delegate to a processor but a processor which goes beyond its mandate will assume the role of a (joint) controller. It notes that the fact that a party offers and contracts for processing services on standard terms does not mean that the party ceases to be a processor. It also notes that the fact there is no written contract does not mean the party is not a processor, just that the contract requirements have not been met.

A further eleven case studies are included in this section which illuminate the line between controller and processor.

It also touches on the fact that in many cases there are multiple processors, and reinforces the message that responsibilities should not be lost along a long chain of service providers. The criticism seems not to be the chain as such but the potential loss of proper control that the use of such a chain may involve.

The data controller should ensure that it is aware of the main elements of the processing such as guarantees for processing in third countries and appropriate security measures through the chain.

Conclusions

The paper ends with a short summary which largely repeats the introduction but places added emphasis on the worked examples and case studies drawn from the experience of different regulators.

Comments and practical application

The important commercial question will always be to assess where liability for any breach lies. This is even more critical now that data controllers can be fined up to £500,000.00 for a breach. The view in the Opinion that joint control does not automatically engage joint and several liability and that each party is separately responsible for its own processing will be welcomed by data controllers.

The Opinion does not explore whether joint and several liability would be assumed where the parties are "co-controllers" that is in those rare cases where they jointly determine the purposes and means of processing for one common processing operation. However this would seem to be the one circumstance where joint and several liability might reasonably be assumed.

The commercial message must be that parties engaged in operations where there is "plurality of processing" should aim to agree clearly at the start of the operation which party is responsible for which aspects of the processing. Often we see contracts with bland and circular clauses which simply assert that each party is responsible for the personal data for which it is data controller but with no allocation of specific responsibilities; businesses should look critically at such clauses in the future.

Working through the various "tests" we have drawn out from the Opinion the following points for parties to consider when faced with a situation of uncertainty over the position:

1. Do any legal obligations apply to the processing and if so on whom do they fall?
2. Which party or parties are most able to deal with the rights of individuals and ensure compliance with the substantive data protection obligations?
3. Do any contractual terms cover any aspects of control of the personal data?
4. Are there overlapping rights which might be relevant e.g. IP rights in a database?
5. What degree of actual control is exercised by each party?

6. Is the processing for the benefit of the party and used for its own purposes?
7. What is the understanding of the data subjects and what impression have they been given as to the identity of the controller?
8. Where does responsibility for accuracy and security of the personal data lie?
9. Who determines the "real" purpose and use of the data?
10. Where the system is an "agreed" industry system is there joint control of the system? Is an industry group running it or are joint decisions made on any aspect of the system or as part of its use?
11. Is the personal data in the system simply passed between users in a chain but never amalgamated or changed?
12. What level of instruction is given to the service provider and what margin of manoeuvre does the service provider have?
13. How far is the service provider monitored?
14. What is the expertise of the parties? Is the service provider using such specific skills that it becomes the controller?
15. How much autonomous decision-making power does the service provider have?
16. Does the service provider provide only a platform which offers functions agreed by the users and would the service provider be able to alter those functions without the agreement of the users?
17. Where are users based? Are they are in different parts of the EU and subject to different data protection laws?
18. What are the privacy risks to individuals and how can those individuals best be safeguarded?

It is suggested that any data protection officer wrestling with one of the knottier questions about the role of a party should work through these. Although not all will be relevant in all cases they should help draw out the issues for further discussion.

© Pinsent Masons LLP 2010

Should you have any questions please contact [Rosemary Jay \(rosemary.jay@pinsentmasons.com\)](mailto:rosemary.jay@pinsentmasons.com) or your usual Pinsent Masons adviser who will be able to assist you further.

This note does not constitute legal advice. Specific legal advice should be taken before acting on any of the topics covered.

LONDON DUBAI BEIJING SHANGHAI HONG KONG SINGAPORE

OTHER UK LOCATIONS: BIRMINGHAM BRISTOL EDINBURGH GLASGOW LEEDS MANCHESTER

T 0845 300 32 32

"Pinsent Masons LLP is a limited liability partnership registered in England & Wales (registered number OC333653) and regulated by the Solicitors Regulation Authority. A list of the members of Pinsent Masons LLP is open for inspection at its registered office address which is CityPoint, One Ropemaker Street, London EC2Y 9AH, United Kingdom. Singapore location in association with MPillay. We use 'Pinsent Masons' to refer to Pinsent Masons LLP and/or affiliated entities that practise under the name 'Pinsent Masons' or a name that incorporates those words, as the context requires". For important regulatory information please visit: www.pinsentmasons.com



Pinsent Masons

www.pinsentmasons.com