



Data Privacy Detective Podcast – Episode 16 – Lawful Processing of Personal Data under the GDPR

Apr 10, 2018

Categories:

[Blogs](#)

[Podcast](#)

[Publications](#)

[Technology Blog](#)

Authors:

[Joseph J. Dehner](#)

“Processing” is defined very broadly by Article 4.2 to encompass a wide variety of ways in which personal data are held or used.

Article 6 describes what constitutes “Lawfulness of Processing.” It lists six alternatives for when processing is lawful. The first and most basic is if “the data subject has given consent to the processing of his or her personal data for one or more specific purposes.” Express consent is at the heart of the European approach to personal data protection. But consent is not the sole basis for lawful processing of personal data.

Article 6.1(b) allows a processor to use personal data to do what “is necessary for the performance of a contract to which the data subject is party” or “to take steps at the request of the data subject prior to entering into a contract.” So, if an individual orders goods or services and provides name, address and payment details, such data can be processed by the seller to consider, accept and fulfill the order.

Consider a job applicant. A French resident applies for a position with a U.S. company that has operations in the EU and elsewhere. What does the company do? Consent to the company’s consideration of the application is implicitly obvious when an unsolicited application is received. The company can consider the application and there will be “processing” to do that. Say the U.S. business approves the hiring of the person to work at the French subsidiary. Then the first part of 6.1(b) comes into play when an employment agreement is created. It should address what data will be collected and used in connection with employment. With clear wording in the employment contract, the company can comply with the rules on how data are processed for such purposes as depositing funds into a bank account or providing benefits.

Recitals that accompany the GDPR's Articles explain the approach. Recital 39 begins vaguely, "Any processing of personal data should be lawful and fair," and this is followed by specifics focused on transparency – requiring that the data subject be informed about how the personal data will be used, stored, corrected when in error and otherwise protected.

Recital 40 puts the focus on express consent of the data subject for applicable personal data that a business obtains and uses. "[P]ersonal data should be processed on the basis of the consent of the data subject concerned" – but there's an escape route – "or some other legitimate basis, laid down by law," meaning by the GDPR or by EU or member state law, "including the necessity for compliance with the legal obligation to which the controller is subject or the necessity 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." So, a business holding personal data can use the information to comply with its (or the controller's) legal obligations, including carrying out contractual duties.

A third alternative to establish lawful processing is if the "processing is necessary for compliance with a legal obligation to which the controller is subject." This is aligned with another alternative at Article 6.1(e) – processing "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller." These alternatives recognize that natural and legal persons can have duties imposed by law to have and process personal data to meet their legal obligations. Article 6.3, however, limits the extent of these alternatives by providing that the basis of processing under these two alternatives "shall be laid down by" EU law or member state law to which a controller is subject. As worded, this alternative would not provide a lawful basis for processing if a business is subject to a requirement imposed by law of a non-EU jurisdiction (unless EU or a member state law so provided). This could create disputes when a non-EU business is required to handle data in a certain manner to comply with its home country laws (e.g., document retention for a fixed number of years), but EU and member state laws do not so provide.

A fifth alternative is if processing is “necessary in order to protect the vital interests of the data subject or of another natural person.” Recital 46 warns that this is a provision of last resort – to be applied only when no other alternative exists for lawful processing. It offers examples such as using personal data in connection with responding to disasters and monitoring epidemics.

The sixth alternative is the least explicit – when 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.

This may serve as a “catch-all” provision for businesses that do not obtain express consent for uses of personal data. Recital 47 offers examples of how this alternative can be used, including that lawful use “could exist ... in situations such as where the data subject is a client or in the service of the controller.” Direct marketing is another mentioned example of an interest that “may be regarded” as legitimate. But the wording of this alternative requires a balancing of the controller’s interest against the data subject’s interest, and so is not a clear and definite basis for establishing lawful processing.

The lawfulness of processing is the starting point for whether personal data can be gathered and processed. Personal data must also be processed “fairly and in a transparent manner in relation to the data subject.” Article 5.1. Considering these principles with the limited instances in which lawfulness can be established without the consent of the data subject means that the surest means of ensuring that processing is lawful is to obtain the consent of data subjects for the particular uses of personal data governed by the GDPR. The next podcast summary will explore how consent can be obtained and documented.

[Click here](#) for access to a comprehensive free database about the GDPR. This is offered by PrivacyRules, an international alliance of technology and law firms dedicated to personal data privacy protection and compliance. The Data Privacy Detective is honored to serve as its Chairman.

For instant access to the GDPR Recitals and Articles, [click here](#), and for more information, please contact [Joe Dehner](#) or any attorney in Frost Brown Todd's [Privacy and Information Security Law Industry Group](#).

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.