PRIVACY INTERNATIONAL

A Guide for Policy Engagement on Data Protection

PART 5:

# Grounds for Processing of Personal Data

# Grounds for Processing of Personal Data

A data controller or processor must identify the legal basis by which their processing of personal data is permitted.

The grounds for processing personal data should be limited and clearly spelled out in law (i.e. there should not be vague, broad grounds, or open list of possible grounds for processing.) Too often, however, laws provide for many grounds.

**Grounds for Processing of Personal Data**

- consent of the data subject
- ensuring the necessity of the processing for the performance of a contract with the data subject or to take steps to enter into a contract
- for compliance with a legal obligation
- to protect the vital interests of a data subject or another person
- for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Some of these are discussed below in more detail.

## Consent

Consent is a core principle of data protection which allows the data subject to be in control of when their personal data is processed: it relates to the exercise of fundamental rights of autonomy and self-determination.

Consent must be freely given, specific, informed, and unambiguous, and can be a written statement, including by electronic means. It should be explicit and require an active process for the individual, rather than a passive opt-out process: as such, it requires positive affirmative action. The entity processing the data must be able to demonstrate they sought and received consent.

Consent is not the only legal ground for processing. In fact, in many situations where there is a power imbalance between the individual and the processor (e.g. between employee and employer), consent cannot be freely given and therefore another legal ground must justify the processing of the personal data (e.g. performance of a contract.)

*Explicit, freely given and unambiguous*

The definition of consent should reflect individual's free and informed choice. For example, the GDPR contains the following definition:

> **'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.**

**Exemptions for Public Institutions**

**In some jurisdictions, notice and consent are not required when the processing is undertaken by a public institution during the exercise of its legal functions. This is the case in Colombia in Article 10 (a) of Law 1581 of 2012, which regulates the processing and management of personal information.**

**It is crucial that such processing is subject to suitable and specific measures to protect the rights and freedoms of individuals.**

*Implied consent*

Some texts may include the concept of implied consent. This was the case in the draft bill proposed for the amendment of the data protection law in Argentina. Privacy International does not believe that 'implied' consent meets the standards of specific, freely given, informed and unambiguous consent.

The Article 29 Working Group (the Group of European data protection authorities) has studied the question of consent, and in particular implied consent, and concluded that implied consent would "not be apt to the GDPR standard of consent."[1]

Particular attention must be given to such a provision to ensure there are clear guidance and conditions as to the contexts in which implied consent would be sufficient.

*Withdrawing consent*

Data subjects should have the right to withdraw their consent at any time. Prior to collecting data, a data controller should be obliged to inform the data subject (at a point prior to obtaining consent) of their right to withdraw consent. This provision should include that any revocation of consent should lead to deletion of the personal data. Consent should be as easy to withdraw as it is to provide. The data controller should take positive action to confirm with the individual that their request has been processed, their consent withdrawn, and their data deleted.

Reliance on consent should not negate the obligation on data controllers to comply with the data protection principles including transparency, fairness, purpose limitation, and data minimisation. Even when relying on consent, data controllers should carefully consider (for example through a data protection impact assessment) any prejudice to the rights of individuals as a result of the processing, and take steps to mitigate these.

**Public Interest**

Another legal ground which is often recognised in data protection laws is the need for processing of personal data if the controller undertakes it in the public interest.

A key consideration here is that data protection law may not define what constitutes 'public interest' and will instead defer to those processing the data or the data protection authority to make that determination. The lack of definition, and clarity around what constitutes 'public interest' and its often-broad interpretation, raises concern that it can act as a loophole.
A public interest ground should be clearly defined to avoid abuse. For example, it should be possible to list the specific public interest grounds (e.g. administration of justice) and ensure that such a list is clear and exhaustive.

If there is to be a condition which permits processing of data in emergency situations, this should be carefully thought through and defined. All grounds for processing should be subject to other safeguards to protect the rights and interests of the data subject, including fairness, transparency and a data protection impact assessment which clearly takes into account any prejudice or adverse effect on individuals.

**Therefore, recommendations for the data protection authority could include:**

- Mapping legislation which include 'public interest' provisions to clarify what these could be
- Requesting that further guidance and a 'public interest' test be developed by the independent supervisory authority
- Requiring public authorities to state clearly what they consider the public interest to be
- If it is to be applied to allow for the processing of sensitive personal data, the independent supervisory authority must define in advance the high threshold of 'public interest' that needs to be met before sensitive personal data can be processed without consent or another legal basis

## Legitimate Interest

Often data protection frameworks, will provide that where a legitimate interest can be demonstrated by the data controller, it may constitute a legal basis for data processing. Given the wide scope of the term legitimate interest it is essential that this condition is qualified. For example, the data controller must also demonstrate that: the processing is necessary and proportionate to the legitimate interest pursued and, it does not override the rights of the data subject.

This condition can be interpreted widely and is open to abuse. Its inclusion in legislation should be avoided if possible.

If this provision is included and there is any doubt in the balancing exercise that there is prejudice to the individual, then the presumption should be that the processing should not go ahead. Furthermore, it is imperative that data controllers provide clear notice to the individuals of the specific legitimate interest they are relying on (i.e. they cannot simply rely on generic or vague legitimate interest), and allow for assessment of prejudice to individuals on a case-by-case basis, including an opt-in mechanism.

Not all legal grounds for processing are available to all controllers. For example, the ability to resort to the justification of legitimate interest has been limited to public authorities under the GDPR. This means that public authorities cannot rely on this justification when processing is carried out in the course of the performance of their duties, but as a public authority they must identify the public interest and the relevant public task/statutory function.

## Processing of Sensitive Personal Data

When processing sensitive personal data, further conditions must be met. The situations in which the processing of sensitive personal data is permitted should be limited. Where consent is to be relied upon to justify the processing of sensitive personal data, it is extremely important that it is explicit and meets all the consent requirements set out above (i.e. informed, free, specific).

To strengthen the principle of purpose limitation (provided for elsewhere in the law), the provision on sensitive personal data should reaffirm that sensitive personal data cannot be further processed for other purposes or by parties other than those identified in the law.

It is also important that the higher protections extend to data that reveals sensitive personal data, through profiling and the use of proxy information, it is possible for those processing data to infer, derive and predict sensitive personal data without actually having been explicitly provided with the sensitive personal data.

Conditions for processing sensitive personal data must be limited, and care should be taken where conditions are proposed such as 'where the data is manifestly made public by the data subject' (Article 9 of the GDPR). Such an approach raises questions: what does 'made public' mean? How can it be verified that it was made public by an individual, and importantly if an individual has made data public, does that mean that data can be used by anyone for any purpose?

This is particularly relevant in the light of recent developments: the evolution of the open data movement and public transparency laws have meant that there are an increasing number of databases and other registries (i.e. property registries, tax registries, or electoral databases) which hold personal data. The fact that these have been made public (for reasons of public interest, transparency, and accountability) does not mean that the data they hold should be permitted to be used for other purposes than those defined at the point of collection.

Furthermore, Privacy International has ongoing concerns over the use of social media intelligence (SOCMINT) as a technique by law enforcement and other security agencies, which is spreading worldwide. They argue that the use of this data, without being subject to any regulation, judicial authorisation, or independent oversight, is lawful as it does not interfere with the right to privacy, relying only on so-called "publicly available" data. We reject this argument. There are clear and serious privacy implications of processing 'publicly available' data on social networking platforms. The fact that data is publicly available does not justify unregulated and unchecked collection, retention, analysis, or other processing.[2]

*Processing of personal data for scientific, historical, or statistical purposes*

It is sometimes included within data protection frameworks that the processing of personal data for data for scientific, historical, or statistical purposes could be a ground for processing data.

**In order to avoid abuse and wide interpretation of this ground:**

- There is a need for clarity on what the statistical and scientific purposes are. Further detail should be included within the law and/or guidance be developed to define this further.
- Such a ground must not exempt a data controller or processor from all of their obligations, and they should provide for appropriate safeguards for the processing of personal data for these purposes.
- Safeguards could include ensuring that the data will not be used to take decisions about the individuals and that the processing is prohibited if it would cause harm.
- A data subject should still have rights over their data including the right to be informed and the right to object that their data be processed for these purposes.

*Processing of personal data and freedom of expression and to information*

A state must take the necessary measures to reconcile the right to protection of personal data with the right to freedom of expression and information. This can include processing for journalistic and human rights purposes, and the purposes of academic, artistic or literary expression. In having to do balance these two rights, there may be exemptions and derogations from the obligations and the rights of data subjects.

For journalism purposes, an exemption might apply to the extent that it is necessary for 1) protection of the right to exercise the fundamental right to freedom of expression and opinion for journalistic purposes and 2) the protection of sources. In addition, we would suggest that any such provision be expanded to include other legitimate exercises of freedom of expression, such as investigations carried out by independent non-governmental organisations.

## References

1 Article 29 Working Party, Guidelines on consent under Regulation 2016/769, adopted on 28 November 2017, as last revised and adopted on 10 April 2018, pp. 30. Available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

2 For more information, see Privacy International's Explainer, available at: https://privacyinternational.org/explainer/55/social-media-intelligence