PRIVACY INTERNATIONAL

A Guide for Policy Engagement on Data Protection

PART 4:

Rights of Data Subjects

Rights of Data Subjects

Right to Information

Individuals must be informed about how their personal data is being processed both where they have provided this directly to a data controller and where the controller has obtained it from another source, i.e. a third party.

Right to Access

Individuals should be informed when their personal data is being collected and they must be able to obtain (request and be given) information about the processing of their personal data.

Right to Object

Individuals should have the right to object to their personal data being processed.

Rights to Rectify, Block and Erasure

Individuals should have the right to rectify, block, and to request the erasure of data processed about them to ensure that such data is accurate, complete, and kept up-to-date.

Rights Related to Profiling and Automated Decision Making

All rights contained in the law should apply to profiling and automated decision making and include the right to request human intervention or to challenge a decision.

Right to Data Portability

Individuals should have the right to obtain all of their personal data from a data controller in a universally machine-readable format or for that data to be ported to another service should they request it.

Right to an Effective Remedy

Individuals should have the right to an effective judicial remedy where they consider that their personal data was not processed in compliance with the law.

Right to Compensation

A person whose rights have been found to be violated has a right to compensation for the damage – material or non-material – suffered.

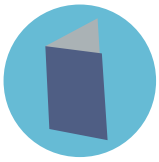
Rights of Data Subjects

A central component of any data protection law is the provision of the rights of individuals, who are often referred to as the data subjects.

These rights should appear early in the law, as they should be seen as applying throughout, underpinning all provisions in the law. These rights impose positive obligations on data controllers and should be enforceable before independent data protection authority and courts.

At minimum, these should include:

- Right to information
- Right to access
- Rights to rectify, block and erasure
- Right to object
- Right to data portability
- Rights related to profiling
- Rights related to automated decision making
- Right to an effective remedy
- Right to compensation and liability.



Right to Information

Individuals must be provided with information about how their personal data is being processed, both where they have provided this directly to a controller and where the controller has obtained it from another source.

Individuals should be provided with at least the following information:

- information as to the identity of the controller (and contact details)
- the purposes of the processing
- the legal basis for processing
- the categories of personal data
- the recipients of the personal data
- whether the controller intends to transfer personal data to a third country and the level of protection provided
- the period for which the personal data will be stored
- the existence of the rights of the data subject
- the right to lodge a complaint with the supervisory authority
- the existence of profiling, including the legal basis,

the significance and the envisaged consequence of such processing for the data subject
- the existence of automated decision-making and at the very least meaningful information about the logic involved, the significance and the envisaged consequence of such processing for the data subject
- the source of the personal data (if not obtained from the data subject)
- whether providing the data is obligatory or voluntary
- the consequences of failing to provide the data

Taking informed decisions and knowing your rights

In order to be able to make an informed decision about whether to use a system or a service and share their data, and so that they can exercise their rights, individuals must be informed when, why, and how their data is being processed.

Functionalities and technicalities of services mean that, on a technical level, a data controller could be processing data without the individual even knowing. For example, some applications are processing vast amounts of data about users, but the user is given little or no information about this, and when they are given information, it is not comprehensible to the average user. In the case of application NaMo, permissions relating to data were not compulsory, and could only be found in the 'Read More' section of the app. Consequently, users were not informed what data the application was processing when downloading the app.[1]

Right to Access

To enable a data subject to exercise and enjoy their rights, and for their enforcement to be effective, the data subject must be able to obtain (i.e. to request and be given) information about the collection, storage, or use of their personal data. The information should include, at least, confirmation of whether a controller processes data about them, the purpose of processing, the legal basis for processing, where the data came from, who it has been/might be shared with, how long it will be stored for, and information about how their data is being used for profiling and automated decision-making. This information should be accompanied by a copy of the requested data.

It is not sufficient merely for the right to be upheld. The law should provide minimum requirements, including for the process of obtaining data relating to those requirements. These include requirements on:

- Timeframe: this should be within a reasonable and stated time.
- Cost: individuals should bear no cost for obtaining information about processing and a copy of their personal data.
- Format: the information provided to the data subject should be in a form that is readily intelligible to them and does not require them to have any particular expertise or knowledge in order to comprehend the information they are provided with.
- Explanation and appeal: if the request is denied, the data subject has a right to be given reasons why, and to be able to challenge such denial. Furthermore, if their challenge is successful they must have the right to have the data erased, rectified, completed or amended.
- Clarity: if there are to be any exemptions to this right these should be clearly set out in law and their application explained to the data subject.

Access rights are an important tool for individuals, journalists, and civil society to investigate, review, and expose how personal data is being processed. A clear and prescriptive law is the starting point for the enjoyment of these rights in practice.

Right to access in practice

The right of access is an essential right for individuals to understand what data is being processed about them and how. Accessing their data enables then people to check whether their data is being processed in line with the law and their expectations, whether its accurate and whether they want to take further action, such as exercising their right to object. This can help them uncover why decisions were made and also expose abusive data practices. This could be, for example, in the context of employment, healthcare, education, financial services or online services. At PI we've made access requests to understand how data is processed on cars[2] and how companies such as data brokers use our data in a largely hidden data ecosystem.[3] Access requests have been used to seek to find out about the use of data in elections,[4] dating apps[5] and telecommunication providers,[6] to name a few.

Openness principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual participation principle

13. An individual should have the right:
a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;
c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial.
d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.[7]

Rights to Rectify, Block and Erasure

A data subject has the right to rectify and block (restrict) data processed about themselves to ensure the data is accurate, complete and kept up-to-date and that it is not used to make decisions about them when the accuracy is contested.

An individual should have the right to demand that the data controller correct, update, or modify the data if it is inaccurate, erroneous, misleading, or incomplete.

Individuals also have the right to 'block' or suppress processing of personal data in particular circumstances. Personal data can then be stored but not further processed until the issue is resolved.

Another right included within many data protection frameworks, such as the GDPR, Nigeria, and South Africa, is the right to erasure. A right to erasure permits data subjects in certain circumstances (i.e. when there is no lawful basis for processing) to request that the data controller erase his/hertheir personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. It is essential that provision is made to ensure among other safeguards, that when processing the request, the data controller will considers the public interest of the data remaining available. It is essential that any such right clearly provides safeguards and in particular exemptions for freedom of expression. The construction of this right and how it will play out in the national context must be considered very carefully to ensure that it is not open to abuse.

Rectifying data and the difference it can make

In light of the data-driven decision-making processes being adopted by governments and industry alike, and the automated nature of data processing (where an individual may not know their personal data is being collected), the need to ensure that the data being processed is accurate more important than ever.

If inaccurate medical data is processed, it could lead to individuals not receiving the medical assistance they need. A mistake in a postal address held by a consumer credit reporting agency could lead to an individual's credit score being poorly (albeit incorrectly) rated resulting in their mortgage application being turned down, as occurred with Equifax Inc.[8]

The UN Human Rights Committee, in interpreting the scope of obligations of state parties to the International Covenant on Civil and Political Rights (of which India is a party since 1979), noted its General Comment No 16 on Article 17 of the ICCPR, back in 1989, that:

> **"In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination."**

Right to Object

An individual has the right to object to their data being processed at any point. If the individual objects, the onus must be on the data controller to provide evidence for the need to continue processing the data of that individual, with reasons which override the interests, rights, and freedoms of that individual. Certain rights to object should be absolute, such as in relation to direct marketing.

Implementing right to object: opt-out by default

When it comes to direct marketing, opt-out was previously the standard approach but in Asian countries new restrictions have been put in place: Hong Kong and South Korea have enacted the tougher opt-in requirements, with severe financial penalties for breaches; all of the others (except Singapore and the Philippines) have some direct marketing restrictions.[9]

Right to Data Portability

Every individual should have the right to request that personal data about themselves that is processed by the data controller be made available to them in a universally machine-readable format, and to have it transmitted to another service with the specific consent of that individual. This right is a step towards ensuring that the data subject is placed in a central position and has a full power over his or her personal data.

Rights Related to Profiling and Automated Decision Making

A data protection law should provide effective protection and rights in relation to both profiling and automated decision-making. This should include all of the above rights; additional rights and guarantees apply exclusively to both profiling and automated decision making to address specific concerns related to these ways of processing personal data.

These rights do not need to be dealt with together as this can lead to unnecessary confusion. However, it is important that both are covered in a data protection framework.

Profiling

Profiling occurs in a range of contexts and for a variety of purposes; from targeted advertising and healthcare screenings to predictive policing. Profiling as a process recognises the fact that data can be derived, inferred and predicted from other data. This can be used to score, rank and evaluate and assess people, and to make and inform decisions about individuals that may or may not be automated. Through profiling, sensitive data (i.e. data revealing particularly sensitive traits of an individual, such as race, political opinions, religious or philosophical beliefs; biometric and health data, etc.) can be inferred from other non-sensitive data.

Profiling, just as any form of data processing also needs a legal basis.
The law should require that organisations who profile are transparent about it and individuals must be informed about its existence. Individuals must also be informed of inferences about sensitive preferences and characteristics, including when derived from data which is not per se sensitive. Since misidentification, misclassification and misjudgement are an inevitable risk associated to profiling, controllers should also notify the data subject about these risks and their rights, including to access, rectification and deletion. Individual's rights need to be applied to derived, inferred and predicted data, to the extent that they qualify as personal data.

Profiling in practice: targeted online advertising

Non-consumer facing data companies collect data from different public and private sources[10], both on behalf of clients and for their own purposes. They carry out profiling by compiling, analysing and evaluating information about individuals, placing them into certain categories and segments.

Profiles feed into targeted online advertising which can be invasive[11] and manipulative, and also has the potential to lead to the exclusion or discrimination of individuals. A 2015 study by Carnegie Mellon University researchers, for instance, found that Google's online advertising system showed an ad for high-income jobs to men much more often than it showed the ad to women.[12] The study suggests that such discrimination could either be the result of advertisers placing inappropriate bids, or an unexpected outcome of unpredictable large-scale machine learning. Intentional or not - such discrimination is an inherent risk of targeted advertising and impossible for individuals to detect.

Automated decision-making

As a result of advancements and innovation in technology and the significant increase in data generated, there are new ways of processing personal data. Data is increasingly playing an important role in decision-making.[13]

This a growing reliance on automated decision-making which is making it difficult to interpret or audit decision-making processes, yet can still produce decisions that are inaccurate, unfair or discriminatory.

> **Automated-decision making in practice**
>
> An example is the use of automated risk scores in the criminal justice system. Proprietary software, such as the COMPAS risk assessment system, that has been sanctioned by the Wisconsin Supreme Court in 2016, calculates a score that predicts the likelihood of an individual committing a future crime.[14] Even though the final decision is formally made by a judge, the automated decision made by a programme can be decisive, especially if judges rely on it exclusively or have not received warnings about the risks of doing so, including that the software potentially producing inaccurate, discriminatory or unfair decisions.

Because of the heightened risks to human rights and freedoms and issues such as fairness, transparency and accountability, data protection frameworks may impose restrictions and safeguards on the ways in which data can be used to make decisions. These safeguards should a right not to be subject to certain automated decisions as this is important where these decisions are consequential for individuals, and in particular where they affect their rights.

Individuals should have a right not be subject to purely automated decision-making. It is important that the law frames this right as a clear prohibition of automated decision-making which protects individuals by default. The law may provide for certain exemptions, i.e. as when it is based on a law (e.g. fraud prevention), or when the individual has given their explicit consent. However, any such exemptions must be limited, as well as and clearly and narrowly defined.

The law must be clear as to what kinds of decisions this right applies to. For example, in the GDPR, Article 22 provides rights in relation to solely automated decisions which have legal or other significant effects. The meaning of these concepts is not crystal clear on the face of the legislation and has required guidance – which makes clear that a decision with fabricated human involvement is also subject to safeguards and that examples of legal or other significant effects include: refusal to grant child or housing benefit; refusal of entry at the border; being subjected to increased security measures or surveillance; or automatically disconnection of from their mobile phone service for breach of contract; automatic refusal of an online credit application, ‘e-recruiting’ practices without any human intervention.

Right to human intervention

Even where exemptions allow for automated-decision making, an individual should have the right to obtain human intervention.

Automated decision-making without human intervention should be subject to very strict limitations. This is particularly important in the law enforcement sector, as a potential miscarriage of justice can scar an individual and impact their wellbeing for life.

As noted above, with reference to the guidelines on automated decision-making and profiling by the Working Party 29 (i.e. the body representing all national data protection authorities in the EU, including the ICO which led on the consultation of this document):

> **To qualify as human intervention, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider all the relevant data.[15]**

Right to an Effective Remedy

The law must include the right of an individual to an effective remedy against a data controller and/or data processor, where they consider that their rights have been violated as a result of the processing of their personal data in non-compliance with the law.

A data subject must have the right to submit a complaint to the independent supervisory authority. This reaffirms the need for the independent supervisory authority to have the power to receive complaints from data subjects, investigate them, and sanction the violator within their own scope of powers - or refer the case to a court. The law should also provide for the data subject to take action against a supervisory authority where they have failed to deal with their complaint.
As well as the right to complain to a supervisory authority, individuals should also have access to an effective judicial remedy via the courts. Individuals should be empowered to take action themselves, as well as instructing others (including NGOs) to take action on their behalf.

In addition, an important and effective mechanism for holding those that fail to comply with data protection law to account is collective redress. Often individuals will not have the resources to investigate and uncover non-compliance, draft complaints, and take further legal action. The cost and complexity of the process

can render their redress mechanisms inaccessible and ineffective in practice. Therefore, a collective redress mechanism should allow NGOs with knowledge of data protection to pursue data protection infringements on their own initiative.[16] Specific provision for NGOs to take action is particularly important in the context of legal frameworks where there might be no other mechanism for collective redress in the field of data protection (i.e. injunctive remedies).

Due to power imbalances and information asymmetries between individuals and those controlling their personal data, data subjects remain as unlikely to pursue cases under the new laws in the future as they were in the past, notwithstanding enhanced enforcement rights. Allowing collective redress would be an effective means to strengthen enforcement.

> **An example of access to effective remedy in action**
>
> The German Consumer Federation took Facebook to court over a number of its breaches of current German Data Protection Legislation; the Court judgement of February 2018 upheld the majority of the consumer organisation's claims, including unlawful terms and conditions and consent provisions in its default privacy settings.[17]

Right to Compensation and Liability

A person whose rights are found to have been violated should have a right to compensation for the damage suffered – material or non-material (e.g. distress).

This underlines the need for robust enforcement models to be in place to ensure that any violation can be investigated and acted upon by a relevant authority.

Exceptions

It is very common that there would be a provision providing for exceptions to compliance with certain principles, obligations, and rights. Often exceptions will relate to the processing of personal data by public authorities - in particular security and intelligence agencies.

It is essential to ensure that, where it provides for such exceptions, the law also provides in-depth details on the specific circumstances in which the rights of data subjects can be limited. These provisions should be limited, necessary and proportionate, and be clear and accessible to the data subject. Moreover, these should not be blanket exceptions but must only pertain to certain rights in very specific and limited situations and be clearly set out by the law.

References

1 Krishn Kaushik, 'Narendra Modi App asks for sweeping access: Camera, audio among 22 inputs', The Indian Express, 26 March 2016, available at http://indianexpress.com/article/india/namo-app-asks-for-sweeping-access-camera-audio-among-22-inputs-facebook-data-leak-5111353/

2 Privacy International, Connected Cars: What Happens To Our Data On Rental Cars?, 6 December 2018, available at: https://privacyinternational.org/report/987/connected-cars-what-happens-our-data-rental-cars

3 Privacy International, Uncovering the Hidden Data Ecosystem, available at: https://privacyinternational.org/campaigns/uncovering-hidden-data-ecosystem

4 Jeremy B White, 'Cambridge Analytica ordered to turn over man's data or face prosecution', The Independent, 5 May 2018, available at: https://www.independent.co.uk/news/uk/home-news/cambridge-analytica-ordered-ico-personal-data-david-carroll-a8338156.html

5 Judith Duportail, 'I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets', The Guardian, 26 September 2017, available at: https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold

6 Hilts, A., Parsons, C., and Crete-Nishihata, M., Approaching Access - A look at consumer personal data requests in Canada, CitizenLab, 12 February 2018, available at: https://citizenlab.ca/2018/02/approaching-access-look-consumer-personal-data-requests-canada/

7 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

8 Tims, Equifax Mistake, op. cit.

9 Greenleaf, Asian Data Privacy Laws (OUP, 2014), p. 493

10 Privacy International, How Do Data Companies Get our Data?, 25 May 2018, available at: https://privacyinternational.org/feature/2048/how-do-data-companies-get-our-data

11 For example, targeting of insecure young people, See: Sam Levin, 'Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless'', The Guardian, 1 May 2017, available at: https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens

12 Datta, A., Tschantz, M. C., & Datta, A. Automated Experiments on Ad Privacy Settings, Proceedings on Privacy Enhancing Technologies, 2015(1), 92–112. Available at https://doi.org/10.1515/popets-2015-0007

13 Privacy International, 'Data is power: Towards additional guidance on profiling and automated decision-making in the GDPR', 2017. Available at: https://www.privacyinternational.org/report/1718/data-power-profiling-and-automated-decision-making-gdpr

14 Danielle Citron, '(Un)Fairness of Risk Scores in Criminal Sentencing', Forbes, 13 July 2016, available at https://www.forbes.com/sites/daniellecitron/2016/07/13/unfairness-of-risk-scores-in-criminal-sentencing/#146a7f514ad2

15 Article 29 Working Party on Data Protection, Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01), Adopted on 3 October 2017 As last Revised and Adopted on 6 February 2018, available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

16 For reference in a UK/EU context, see: Anna Fielder, 'Why we need collective redress for data protection', Privacy International Medium, 9 January 2018, available at https://medium.com/@privacyint/why-we-need-collective-redress-for-data-protection-863c6640689c

17 English press release available at: https://www.vzbv.de/sites/default/files/downloads/2018/02/14/18-02-12_vzbv_pm_facebook-urteil_en.pdf