# An Introduction to the GDPR (v2)

By Andrew Cormack, Chief Regulatory Adviser at Jisc



*To comment on this article, please visit our GitHub repository and submit an issue.*

## Table of Contents



## Abstract

The General Data Protection Regulation (GDPR) applies to any processing (including collection, storage, or sharing) of data relating to identifiable (including by serial numbers, IP addresses, etc.) individuals who are physically in Europe. This scope may well cover international or online Identity and Access Management (IAM) activities, as well as all IAM activities actually conducted in Europe. All such processing must conform to seven principles: lawfulness, fairness & transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity & confidentiality; accountability. Individuals have rights of information; subject access; rectification, erasure & restriction. Processing must be for one of six legal bases: contract, legal obligation, vital interests, public interests,

legitimate interests, or consent. Each basis has its own requirements; some confer additional rights on individuals.

## Introduction

The *General Data Protection Regulation (GDPR)*,[i] which came into force in all EU member states on May 25, 2018, applies when processing 'any information relating to an identified or identifiable natural person'.[ii] The inclusion of 'identifiable' makes it much broader than most privacy laws: IP addresses, MAC addresses of personal devices, account numbers, and even unique patterns or combinations of attributes may be sufficient to bring an activity within its scope. 'Processing' is not limited to digital formats: personal information prepared for, or derived from, digital processing is covered, as well as the content of any structured filing system. The range of activities covered is similarly wide: including 'collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or deletion'.[iii] Since the GDPR covers all individuals physically in Europe – there is no citizenship or similar requirement – it is very likely to apply to the international or online activities of organisations elsewhere in the world, as well as to all organisations in Europe.

IAM activities are likely to be regulated by the GDPR; however, effective IAM may make it easier for organisations to comply with the law's requirements. The behaviour it prescribes is increasingly expected, not only in Europe, but in the increasing number of countries subscribing to the Council of Europe's Convention 108.[iv] Within Europe there are significant fines for contravention of the GDPR, but following its principles should have benefits for the reputation and efficient operation of organisations anywhere in the world.

This article is not a complete guide to the GDPR but covers those aspects most relevant to IAM. It first describes the general principles and obligations that apply to all personal data processing; then examines the permitted legal bases for processing and the specific obligations and rights associated with them. Finally, examples show how IAM activities can help organisations conform to the GDPR's requirements.

## Terminology

- **General Data Protection Act (GDPR).** Formally, Regulation 2016/679 of the European Union, in force May 25, 2018. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
- **Personal Data.** Defined in Article 4(1) of the GDPR: "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;". Note: "natural person" (human) is used to distinguish from companies and other corporate entities that are "legal persons".
- **Processing.** Defined in Article 4(2) of the GDPR: "'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation,

structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction". Note that even this long list of activities is not exhaustive: other activities may also fall within the definition of "processing". Additional rules, in Article 22, apply to "automated individual decision-making, including profiling". These generally have the effect of strengthening the rights of information and objection described later and may limit the use of automation for some high-impact decisions.

- **Special Category Data (SCD).** Categories of data that are regarded as particularly sensitive, so subject to additional regulation. Defined in Article 9(1) of the GDPR as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"; Article 10's "personal data relating to criminal convictions and offences" requires similar treatment, so is normally considered as another category of SCD.
- **Data Controller.** Defined in Article 4(7) of the GDPR: "'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;".[v] This article uses the term "organisation" as a synonym for "data controller", since organisations involved in IAM will normally be data controllers.
- **Data Processor.** Defined in Article 4(8) of the GDPR for situations where an organisation processes personal data solely on the instructions of others. A Data Processor must not determine the purposes of processing, for example by processing in its own interests, or, beyond limited technical choices, the means of doing so. Data Processors are regulated by Article 28: in particular they must have a contract with the Data Controller that covers all the subjects listed in Article 28(3). Data Processors are excluded from some, but not all, of the liabilities and duties of Data Controllers.
- **Data Subject.** Defined in Article 4(1) of the GDPR (see "Personal Data" above) as the formal term for the human to whom personal data relates. This article uses the term "individual" as a synonym for "data subject".

## Rules for Personal Data

The GDPR places most of its obligations on organisations that "determine[…] the purposes and means of the processing of personal data" (Art 4(7)): these organisations are referred to as *Data Controllers*. Some organisations may process data solely on behalf of others – not determining the purposes and means – these are known as *Data Processors* and have fewer obligations. Since IAM systems are likely to act as data controllers, their main obligations are described here. The fundamental obligations on all data controllers are to act in accordance with seven principles, and to satisfy obligations to, and rights of, individuals ("*data subjects*") whose information they process.

### Principles (Art 5)

According to GDPR Article 5, the following principles apply to all processing of personal data:

- **Lawfulness, Fairness, Transparency**: all processing must be covered by one of the six legal bases set out in the GDPR (see below) and must not breach other laws; it should not be deceptive, any activities that individuals might be surprised by should be explained and justified as must any adverse effects on individuals; organisations should be open about their processing, in particular through the rights to information and subject access described below.
- **Purpose Limitation**: the purposes for which information is processed must be clearly stated; existing information may only be used for new purposes if, either, the new purpose is compatible with the existing ones (roughly summarised as 'not surprisingly different'), or it is required by law, or each individual has given consent to the new purpose. IAM systems should be designed to serve a single purpose and any proposals to re-use their data for other purposes should be reviewed for compatibility with that purpose and with the information provided to users.
- **Data Minimisation**: the data and processing must be relevant to the purpose, sufficient to achieve it ("adequate"), but not excessive. Well-defined IAM systems should contribute to data minimisation: for example, federated systems can reduce disclosure by using opaque identifiers ("pseudonyms") that allow an individual to be recognised when they return to a system, without identifying them. IAM systems should be designed to collect, use and disclose the minimum personal data required for each function. If a function can be delivered with anonymous or pseudonymous data, then it should be. This is the basis for Data Protection by Design, discussed in GDPR Article 25.
- **Accuracy**: personal data must be accurate and up to date. Although individuals have the right to correct errors in their data (see "right of rectification" below) organisations should not rely on them doing so as the sole, or even principal, way to ensure accuracy. IAM systems that act as a single source of truth for their organisations should make accuracy significantly easier to achieve; those that do not should be accompanied by appropriate policies, processes and workflows to ensure that their information is, and remains, accurate.
- **Storage [time] Limitation**: personal data must not be kept for longer than needed for the stated purpose(s). Before collecting personal data, organisations should know, and declare, how long they will keep it for, either in relation to a fixed time period (e.g., 'six months'), or a known event (e.g., 'until you leave'). Organisations should have processes to ensure their stated retention periods are implemented; at the end of them data should be deleted or anonymised. The purposes of archiving, research, and statistics may allow personal data to be kept for longer, but subject to specific conditions in both European and national laws.
- **Integrity and Confidentiality**: organisations must use appropriate technical and organisational controls to protect the security of personal data. What is appropriate will depend on the sensitivity of the data and the purpose: it is likely to change both as new protective technologies and approaches become available and as new threats and risks become apparent. The GDPR imposes specific obligations if there is a breach of security, which are described below. IAM systems should help both by holding their own personal data securely, and as a component of the access control systems used to prevent unauthorised access to personal data elsewhere in the organisation.

- **Accountability**: organisations must be able to demonstrate that they are complying with the principles and other requirements of the Regulation. This will normally require both documentation showing that these principles and requirements were considered in the design of the system, and audit logs (which themselves may contain personal data) confirming that normal operations and responses to events such as breaches and any exercise of individual rights were, in fact, conducted in accordance with them.

### Obligations and Rights

Three groups of "rights" apply to all processing of personal data except where limited exceptions, set out in the specific Articles, apply. The first group creates an obligation on organisations towards all those whose information they process; the second and third require organisations to have systems to handle requests from individuals who exercise their rights:

- **Rights to Information**: to support the above Principles, organisations are required to provide at least a minimum set of information to all those whose personal data are processed: who the organisation is, what data are being processed, why, for how long, whether automated decisions are involved; any other organisations or further processing involved; how to exercise your rights. Article 13 applies when data are collected directly from the individual; Article 14 when an organisation obtains personal data from another source (including public sources).
- **Subject Access Right**: individuals have a general right, under Article 15, to ask and be told whether their data are being processed, what data, why, for how long, whether automated decisions are involved; the source of the data and any recipients; how to exercise their rights. In addition, if this can be done without affecting the rights of others, the individual has a right to receive a copy of their own data. Determining what to release, and when, can be complex, especially when the requester's identity may be uncertain. IAM systems built around guidance from regulators[vi] can reduce the risk of error or fraud.
- **Rights of Rectification/Erasure/Restriction**: Article 16 ("rectification") entitles individuals to correct inaccurate personal data, including to add additional information. Article 17 ("erasure") entitles individuals to have their personal data deleted if there is no lawful basis for it to be kept. This might arise, for example, when excessive information is held, if it has been kept beyond its retention time, or, if it was being processed on the basis of consent (see below) when that consent has been withdrawn. Article 18 ("restriction") entitles an individual to block further processing of their data (including deletion) while a rectification or objection right is being processed, or as an alternative to erasure if the individual needs the data for a legal claim. IAM systems that provide a single point of truth and control should make it easier to implement these rights.

## Legal Bases for Processing

To be lawful, any activity that involves processing personal data must be covered by one of the six legal bases set out in Article 6 of the GDPR. Note that the basis applies to a particular processing activity, not to a dataset. As illustrated in the example below, an IAM system may involve several different legal bases. While IAM professionals should probably not be determining the Legal Bases on behalf of their organisations, they need to be aware of the implications of that choice.

Various types of personal data – including race, ethnicity, and health – are considered higher risk and processing must be for one of the purposes set out in Article 9, as well as having an Article 6 basis. The requirements on processing these types – known as *Special Category Data* – are often set in national, rather than European, legislation. IAM systems that process them should therefore consult lawyers familiar with the relevant national

schemes. Similarly, although the GDPR highlights the extra risks involved in children's personal data, the specific additional requirements – including the age below which someone is considered a child – are largely set at national level, so are not covered here.

Each of the Article 6 bases imposes additional conditions on processing, both by its definition and, in some cases, by explicit additions. Several of the bases also create additional obligations for organisations processing personal data and/or rights for individuals whose personal data are processed. The following sections describe these legal bases; here they are set out in the likely order of preference for organisations, rather than that in which they are listed in the legislation; those at the bottom of the list are significantly more onerous.

### Necessary for the Performance of a Contract

Five of the legal bases begin "necessary for…". Regulators have confirmed that this means there must be no less intrusive way to achieve the purpose.

The inclusion of "performance of" indicates that there must be a particularly close link between the processing and the subject of the contract; the individual whose data are processed must also be a party to the contract. However, the term "contract" is likely to be widely interpreted, covering many situations where parties have made an agreement, even without a formal contract document. If stopping processing would make that agreement impossible to fulfil, then "necessary for contract" may well be an appropriate basis. This is likely to apply to many IAM systems, for example those provided for internal use by an employer or educator. Even for stand-alone IAM systems – so long as there is a direct relationship between the individual and the IAM provider – using "necessary for contract" may be a useful way to distinguish the minimum data and processing without which the service cannot function from optional data that the system can use but does not need. The latter should use the basis of "consent" described below. The European Data Protection Board's Guidelines clarify that ancillary functions including service improvement, fraud prevention and online behavioural advertising are likely to need a different legal basis[vii].

Where personal data are processed on this basis, the GDPR introduced a Right to Portability (Article 20) covering data "which [the individual] has provided". This right may therefore cover only a subset of the information available under the general Subject Access Right, though the information must be provided "in a structured, commonly used and machine readable format". So far, Regulators have only provided high-level guidance on this right,[viii] including suggesting that CSV might fulfil the format requirements, so further developments are likely.

### Necessary for Compliance with a Legal Obligation

Where a European or Member State law requires an organisation to process personal data, this is likely to be the appropriate legal basis. It is possible that this might apply to some national IAM schemes, and those in regulated industry sectors, but otherwise it is unlikely to be relevant.

### Necessary in Order to Protect Vital Interests

This legal basis may apply when there is a threat to life or serious injury. We should hope that it is not relevant to our IAM systems!

### Necessary for the Performance of a Task Carried out in the Public Interest

This legal basis is typically used where a law permits processing for a public interest task but does not require it. Since national, and other statutory, IAM schemes will normally be subject to a legal requirement (see "legal obligation" above), rather than a permission, it seems unlikely to be relevant to IAM systems.

This basis gives individuals the Right to Object to processing, as described under "legitimate interests" below.

### Necessary for the Legitimate Interests of the Controller or a Third Party

Whereas the first four bases cover specific situations defined in law the last two ("legitimate interest" and "consent") are more flexible and are therefore subject to more onerous requirements to protect individuals. This Legitimate Interests basis requires not just that the processing be necessary to achieve a specific purpose (the "interest") but also that that interest be "legitimate" and, uniquely, that the benefits of processing not be overridden by its risks to individuals. A processing activity may be necessary for a legitimate interest, but still be unlawful if it cannot satisfy this balancing test.

Legitimate interest will, however, often be the most appropriate legal basis for multi-lateral IAM, for example where identity assertions are provided to external organisations ancillary to a contract for some other purpose. Organisations participating in federations – whether as identity providers, service providers, attribute authorities, or otherwise – are unlikely to know enough about the user's reason for making a particular request to know whether it is necessary for a contract or, conversely, a situation where the individual is able to give free consent. Rather than trying to communicate that information among multiple parties or establishing a mesh of contracts among them, it is often simpler to consider the interest of each individual organisation in providing the service that the individual – by initiating an authentication or authorisation process – has requested of them.

This basis can only be used if "such interests are not overridden by the interests or fundamental rights and freedoms of the [individual] which require protection of personal data" (Article 6(1)(f)). Before an IAM organisation considers releasing (or requesting) information on this basis, it must therefore consider what risks might arise to the individual as a result of that disclosure. The mention of "fundamental rights and freedoms" indicates that risks beyond just data protection should be considered. Although this might appear onerous, the process can often be simplified, and implemented in the form of attribute release policies, by considering the types of data involved and what is known about the entities that will receive the information. Releasing a low-risk attribute to an organisation that has committed (or is required by its own applicable laws) to only use such data for service provision might be considered an acceptable risk, given that the individual must first have chosen to request federated authentication to that organisation's services.

When using the legitimate interests basis, each individual has a "Right to Object" under Art.21. The legal requirement is to consider whether the organisation has "compelling legitimate grounds" for continuing the processing, in which case it may do so. In practice, since IAM systems should, in any case, only be processing the minimum information necessary to provide their service to users, an objection is effectively a request to stop using those parts of the service that rely on Legitimate Interests. An organisation might, therefore, respond to such a request by checking that that is, indeed, the individual's intention.

### Consent

The only legal basis that does not contain the word "necessary" is that the individual has given consent to processing. However, this is subject to significant conditions – in Article 7 and Recitals 32, 42 & 43 – which are likely to make consent inappropriate for much of the processing involved in IAM. Consent must be indicated by "a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the [individual's] agreement"; it must be possible to withdraw consent at any time, as easily as it was given; consent will not be valid "if the [individual] has no genuine or free choice or is unable to refuse or withdraw consent without detriment". Consent might be used where an IAM system can contain additional information, or support other processing, that is not necessary for its core function (for example nicknames), but in this case the individual has an absolute right to have that additional information removed, or the extra processing terminated, at any time.

In addition, consent sought by an employer, public authority, or other organisation with similar power over the individual is presumed not to be free. Consent must not be sought as a condition of providing a service. Organisations relying on consent must be able to demonstrate that it was obtained in accordance with these conditions. As for "contract" above, the Right to Portability applies to information obtained using consent.

### Summary

The "necessary" bases – usually either contract, legitimate interest, or legal obligation – are more suitable for the information necessary to maintain the relationship between the individual and the IAM system. With these, the organisation does not have to worry whether lawful consent was obtained, nor that it might be withdrawn on a whim. Consent should be reserved for information that the IAM system can handle but does not need: circumstances that are much more likely to satisfy the requirements for it to be valid. Consent, according to the UK's Data Protection Regulator, should be an offer to the individual to enter into a deeper, more trusting, relationship.[ix]

### International Transfers

Any transfer of personal data from a country within the European Economic Area to one outside (commonly referred to as an "export") requires its own legal basis. The full list of possible bases can be found in Articles 45-49. In practice, and unlike the previous Data Protection Directive, it will usually be possible to use the same legal basis for international IAM operations as those within Europe: regular transfers of personal data (for example between a customer organisation and a non-European IAM supplier) should normally be

covered by a contract including one of the sets of Standard Contract Clauses;[x] occasional, ad hoc, low-risk transfers should be able to use the legitimate interests basis; consent may be used where the individual is free to choose whether or not their personal information are transferred. Arrangements for international transfers are subject to change: for example both the original US Safe Harbor scheme and the Privacy Shield that replaced it have been declared invalid by the European Court of Justice; the latter case ("Schrems II") also added new obligations for exporting organisations using the Standard Contract Clauses, with new versions of the Clauses currently being proposed by the European Commission. Organisations operating international IAM systems should be aware of developments.

## Security

As well as requiring organisations to take proactive measures to protect the security of personal data, Article 33 of the GDPR introduces significant reporting requirements when an organisation becomes aware of a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". The wide definition of "breach" and the inclusion of "accidental" means that organisations should be particularly careful when designing, testing, and documenting processes that may alter, delete, or disclose data. All such breaches must be reported to the Regulator unless they are "unlikely to result in a risk to rights and freedoms of natural persons". Loss of an encrypted memory stick, while the decryption key remains secure, is often given as an example of a breach that may not need to be reported. The expectation is that such reports will be sent within 72 hours: if not, then a satisfactory explanation for the delay must be included. Where a breach is likely to involve a "high risk" to individuals' rights and freedoms, then a notification to affected individuals is required under Article 34.

The GDPR recognises in Recital 49 that the ability to detect, contain, and remedy security breaches is an important part of keeping data secure. Indeed, it has been suggested that failure to do so may itself be a breach of Article 33.[xi] Processing of personal data such as access and activity logs required for those purposes is recognised as a legitimate interest (so permitted, subject to the balancing test). Such logs must, of course, be held and processed securely. IAM can play a significant role in mitigating security breaches, by disabling compromised accounts quickly and effectively; its logs may also provide early warning when an organisation is under attack.

To meet the GDPR's tight timescale for understanding and reporting breaches, organisations must plan, prepare, resource, and practice how they will respond to security incidents. This could include assessing which types of breach of the IAM system would require notification to regulators, individuals, or neither, as well as identifying and establishing contact with the internal and external partners whose help would be required.

## IAM Examples

The following examples show ways that IAM systems can support the GDPR.

### Example 1: Outsourced Office Systems

John works at a small business, which has contracted with a cloud service provider to run its HR and office software services. As agreed in that contract, the service provider

subcontracts the operation of email and document sharing to Google. John's employer enters the information necessary for his employment role into a series of webforms; the service provider sets up the necessary accounts and document permissions. John's personal data is processed on the basis that it is necessary for his contract of employment; only the information required to set up his email and document account is passed to Google.

In this example, John is the Data Subject and his employer is the Data Controller. Provided they only use information to provide the contracted services, the service provider and Google are Data Processors. If either were to use data for their own purposes – for example, to display customised adverts – then they would be Data Controller for that processing and be required to fulfil all the Data Controller's obligations.

### Example 2: Federated Access Management

Janet is a professor at the University of Erewhon. The university has a central IAM system containing the details of all staff required for them to do their jobs. This information is stored and processed on the legal basis that it is necessary for Janet's contract of employment with the university: without doing so, it would be impossible to perform that contract. The IAM system acts as a single point of truth, so ensuring that information is up to date throughout the university and that any correction requests can be easily implemented.

The IAM system also allows Janet to store optional information, such as her personal interests, that will appear on her staff webpage. Since she can add, change, or remove these at any time, without affecting her work, the appropriate legal basis is consent.

The university is also a member of an Authentication & Authorisation Infrastructure (AAI) Federation. When Janet accesses a website of another Federation member (for example, a journal publisher), she can choose to log in with her university credentials. A wide variety of organisations are Federation members since – with the university taking responsibility for providing verified information and ensuring its users' good behaviour – this allows them to receive and process considerably less personal data, in accordance with the data minimisation principle. Janet needs to access some of these for her work, but others may be just for personal interest. Since neither the university nor the sites wish to work out which sites are necessary for contract and which accessed with free consent (where Janet needs to access a site for work, her consent cannot be free) they both use the legal basis that the processing is necessary in their legitimate interest in helping Janet access the information she wants.

The legitimate interests basis requires the university to balance the risks of releasing information against the benefits. Since the federation agreement requires members only to use authentication and other attributes for the purposes of service provision and personalisation, and not to attempt to identify pseudonymous users, the university assesses that there is very little risk in releasing a unique opaque identifier and Janet's status as a member of staff to any Federation member; it has therefore configured its systems to release that information by default when a user requests a federated login. This is sufficient both for Janet to access online journals, and to verify her entitlement to a staff discount at the local health club.

The Federation has defined a class of services that are specifically designed for Research and Education use, and that require a name and email address in addition to the opaque identifier and status. This additional requirement is mentioned in the services' privacy notices. Although this disclosure involves a slightly higher risk, the university is satisfied that this is justified by the greater benefit; such services will therefore receive the additional information by default. This allows Janet to use discussion groups and virtual research environments in her field.

Where services ask for more information, the university will perform an individual assessment of the benefit and risk. This may indicate that additional measures, such as a bilateral contract or the free consent of each individual, are required to reduce the risk of the disclosure.

In this example, Janet is the Data Subject. Both the university and the service provider are Data Controllers, since the service provider chooses which services to offer to Janet.

## Author Bio

Andrew Cormack is Chief Regulatory Adviser at Jisc. He has been involved in the technical and policy development of federated identity systems in the UK, Europe, and globally for more than fifteen years. He has spoken and written extensively on how digital technologies can be used to improve privacy and data protection and, more recently, on the application of the GDPR to them. His publications can be found at https://orcid.org/0000-0002-8448-2881 and his blogs at https://community.jisc.ac.uk/blogs/regulatory-developments.

## Change Log

| Date | Change |
|---|---|
| 2021-06-30 | Updated based on https://github.com/IDPros/bok/issues/42, https://github.com/IDPros/bok/issues/41 |

[i] "EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," OJ 2016 L 119/1.

ii GDPR Art.4(1)

[iii] GDPR Art.4(2)

[iv] "Council of Europe Data Protection website," Council of Europe, accessed October 10, 2019, https://www.coe.int/en/web/data-protection/home.

[v] Note that some public authorities are excluded from GDPR, notably institutions of the European Union itself and law enforcement and national security agencies when performing those tasks. These will normally be subject to other legislation that applies the same principles: for example, Regulation 2018/1725 for EU bodies and Directive 2016/680 for law enforcement.

[vi] See, for example, the UK Regulator at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

[vii] European Data Protection Board, "Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects," Version 2.0, 8 October 2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf.

[viii] "Guidelines on the right to "data portability"," revision (wp242rev.01), European Commission, last modified October 27, 2017, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

[ix] "When is consent appropriate?" Information Commissioner's Office, accessed October 10, 2019, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/#when3.

[x] "Standard Contractual Clauses: Standard contractual clauses for data transfer between EU and non-EU countries," European Commission, accessed October 10, 2019, https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

[xi] "Guidelines on Personal data breach notification under Regulation 2016/679," Article 29 Data Protection Working Party, last revised and adopted on February 6, 2018, https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49827