# CREATING A DATA PROTECTION FRAMEWORK: A DO'S AND DON'TS GUIDE FOR LAWMAKERS

## LESSONS FROM THE EU GENERAL DATA PROTECTION REGULATION


accessnow.org

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

**November 2018**

**This paper is an Access Now publication.**

For more information, please visit: **https://www.accessnow.org,** or contact: **Estelle Masse** | Senior Policy Analyst | **estelle@accesnow.org**

# TABLE OF CONTENTS

## INTRODUCTION

Access Now presents *Creating a Data Protection Framework: A Do's and Don'ts Guide for Lawmakers - Lessons from the EU General Data Protection Regulation to contribute to the global discourse on data protection*. The paper particularly reflects on the European Union's approach to the debate and the level of protection for personal data around the world.

The General Data Protection Regulation (GDPR) of the European Union is a positive framework for users' protection and will help users take back the control of their personal information. While the law is currently being implemented, it is already inspiring governments around the world to upgrade or develop data protection legislation, which brings massive opportunities. There are important lessons to be learned from the negotiations of the GDPR, many positive and some negative.[1] From our experience, we have created a list of do's and don'ts that lawmakers should consider when developing a data protection framework.



## BACKGROUND

Have you ever filed taxes or made a phone call? Do you own a smartphone? Have you ever used the internet? Do you have a social media account or wear a fitness tracker? If the answer is yes to any of these questions, it means that you have been sharing personal information, either online or off, with private or public entities, including some that you may never have heard of. Sharing data is a regular practice that is becoming increasingly ubiquitous as society moves online. Sharing data does not only bring users benefits, but is often also necessary to fulfill administrative duties or engage with today's society. But this is not without risk. Your personal information reveals a lot about you, your thoughts, and your life, which is why it needs to be protected.

The right to protection of personal data is very closely interconnected to, but distinct from, the right to privacy.

More than 160 countries refer to the right privacy in their constitutions, but the understanding of what "privacy" means varies from one country to another based on history, culture, or philosophical influences.[2] This explains why the way to protect privacy might differ from one country to another even if many legal traditions center the protection of privacy on the right to respect for private and family life, home, and correspondence. Data protection, on the other hand, is not always considered as a right in itself. The 28 member states of the European Union are an exception, as they have recognised data protection as a fundamental right in the 2001 EU Charter.[3] However, the protection of personal data is of paramount importance in our

[1] Access Now, General Data Protection Regulation – what tidings do ye bring? https://www.accessnow.org/general-data-protection-regulation-what-tidings-do-ye-bring/
[2] See results provided by the Constitute Project https://www.constituteproject.org/search?lang=en&key=privacy
[3] See Article 8 of the EU Charter of Fundamental Rights, 2001. http://www.europarl.europa.eu/charter/pdf/text_en.pdf

increasingly digital society. It is often recognised through binding frameworks at the national, regional, and international level, and in many places where it is not yet codified, lawmakers are in the process of doing so. We believe this should happen as quickly as possible.

Protecting personal data, or personally identifiable information (PII), means establishing clear rules that any entity that processes your information must follow. This is not a new concept, as data protection laws have been in place in many countries around the world for more than 40 years, but these laws are becoming increasingly important as people are sharing more data and companies' data collection and use skyrockets. The first data protection law was passed in 1970 by the German federal state of Hesse.[4] A few years later, the US developed the "fair information practices" that have influenced modern data protection laws, even though the US has never followed up with a codified legal framework for data protection at the federal level, instead adopting sector-specific laws.[5] Then came the first country-wide laws protecting personal data, in Sweden, Germany, and France, before international organisations such as the Council of Europe adopted international frameworks. The Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data — also known as Convention 108 — was adopted in 1980 and became open for signature in 1981.[6] In 1980, the Organisation for Economic Cooperation and Development (OECD) also developed its privacy guidelines.[7] Since its adoption, the Convention 108 has been ratified by all 47 member countries of the Council of Europe, and by Mauritius, Senegal, Uruguay, and, most recently, in 2017 by Tunisia.[8] The Convention 108 had a pivotal role in the adoption of the first Europe-wide data protection law in 1995.[9] Today, hundreds of countries around the world have adopted general or sectoral data protection laws.[10]

In addition to the frameworks in place, there are countries currently considering data protection legislation: Tunisia, India, Japan, South Korea, Brazil, and Argentina, to name but a few.[11] For some of these countries, it would be their first data protection law. Access Now has worked on data protection legislation across the world since 2009, and in particular, on the EU reform that led to the adoption of the General Data Protection Regulation.[12] The EU and its member states have a long data protection tradition and it is often considered a standard-setter in this area, which means that many countries are interested in replicating the GDPR in their own jurisdictions. There are important lessons to be learned from the negotiations of the GDPR, many positive and some negative. From our experience, we have created a list of do's and don'ts that lawmakers around the world should consider when developing a data protection framework.

[4] Hessische Datenschutzgesetz,Original version dated from 7 October 1970. (GVBl. I S. 625).
[5] See EPIC, the code of fair information practices. https://epic.org/privacy/consumer/code_fair_info.html
[6] Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data, 1981. http://www.coe.int/web/conventions/full-list/-/conventions/treaty/108
[7] See Privacy International, Data Protection. https://www.privacyinternational.org/node/44
[8] Access Now, Tunisia ratifies Convention 108 and affirms commitment to the protection of personal data https://www.accessnow.org/tunisia-ratifies-convention-108-affirms-commitment-protection-personal-data/
[9] Peter Hustinx, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, 2015. https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf
[10] See Privacy International, Data Protection. https://www.privacyinternational.org/node/44
[11] Tunisia national authority for the protection of personal data. Projet de loi relative à la protection des données personnelles, 2017. http://www.inpdp.nat.tn/Projet_PDP_2017.pdf
[12] European Union, Regulation 2016/679/EU 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) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

## DO'S

Below you will find 10 recommendations for policymakers to follow when developing a data protection law. These 10 steps are individually and collectively necessary to ensure open negotiations and the adoption a user-centric framework.

### 1 ENSURE TRANSPARENT, INCLUSIVE NEGOTIATIONS

Governments and decision makers must ensure that negotiations of data protection frameworks are conducted in an open, transparent, and inclusive manner. This means conducting public consultations and expert roundtables, publishing negotiating texts and allowing comments from all interested parties with reasonable deadlines, and providing feedback on received comments. In all stages, meaningful participation from civil society groups must be ensured, and all meetings of decision makers with industry, NGOs, and consumer groups must be made public in an easily accessible registry. Maximum transparency around lobbying should accompany the process. Due weight should be given to input from civil society, to redress the inevitable imbalance in number of voices compared with industry.

**Experience from the GDPR negotiations**

The GDPR negotiations were conducted in accordance with the EU legislative process. This process is fairly transparent and generally ensured the publication of draft proposals, opinions, reports, amendments, and legal opinions of all EU institutions on any piece of legislation being discussed. Some improvements can however be made to this legislative process. First, there should be more accountability in the earliest drafting stage of legislation. Through a FOIA request, Access Now has for instance obtained an email revealing how the Home Affairs department of the European Commission (DG Home) had been working alongside the US administration during the early stages of the privacy reform effort.[13] In addition, the trilogue — the final stage of the negotiations between all EU institutions — is notoriously opaque. Access Now has joined efforts led by European Digital Rights (EDRi) in calling for reforms of the process for years.[14] Because of the lack of transparency during that stage, the public is kept in the dark at the most crucial point in the negotiations; that is, when lawmakers come together to agree on a final compromise text that will become binding after the EU institutions rubber-stamp it.

External stakeholders seeking to influence negotiations should also abide by principles of transparency and accountability. The GDPR negotiations were subjected to an unprecedented lobbying effort during which industry representatives aimed to weaken existing data protection standards and to prevent proposals from strengthening users' rights. The influence of certain industries and foreign companies became visible as lawmakers copied and pasted amendment proposals from lobbying proposals.[15] In that instance, advocacy groups were able to help the public compare the language proposed by lobbyists to the text proposed by lawmakers.[16] This process allowed the public to comment meaningfully on these proposals and helped fight influence via secret backroom dealings. Proposing amendments is not necessarily a shady activity, but it must be done in a transparent manner. People must know where these proposals are coming from and lobbyists should always indicate their affiliation on their proposals and make them available to the public.

[13] Access Now, Big brother's little helper inside the European Commission https://www.accessnow.org/big-brothers-little-helper-inside-the-european-commission/
[14] Access Now, EU "trilogues" consultation: A foot in the door for transparency https://www.accessnow.org/eu-trialogues-consultation-foot-door-transparency/
[15] Access Now, Privacy under siege: Unprecedented lobby efforts against the Regulation are revealed https://www.accessnow.org/privacy-under-siege-unprecedented-lobby-efforts-against-the-regulation-are/
[16] See LobbyPlag initiative http://lobbyplag.eu/compare/overview

## 2 DEFINE AND INCLUDE A LIST OF BINDING DATA PROTECTION PRINCIPLES IN THE LAW

Any framework aiming to protect personal information must include a clear definition of personal and sensitive data. The level of protection should correspond with the sensitivity of each category of data. Sensitive data should be defined to include genetic and biometric data, as well as communications content and metadata, as this information reveals particularly sensitive personal traits. This means that a data protection framework can also include specific measures for the protection of data exchanged during communications and related privacy provisions to guarantee the confidentiality of communications.

Together with clear definitions, the eight following principles are at the core of data protection frameworks.[17] Put together, these interconnected principles lay down the necessary measures that any data protection framework which seeks to effectively protect users' rights should include. The effective codification of these principles requires the development of a set of users' rights, legal basis for data processing, data security measures, oversight mechanisms, obligations for entities processing data, and of measures enabling the transfer of data to third countries.

1. **Fairness and lawfulness:** Personal data shall be processed fairly and lawfully which means that information should be processed on a clear legal basis, for a lawful purpose, and in a fair and transparent manner so that users are adequately informed about how their data will be collected, used, or stored, and by whom.

2. **Purpose limitation:** Personal data shall be collected and processed only for a specified and lawful purpose. This purpose shall be specific, explicit, and limited in time. Data shall not be further processed in any manner incompatible with that purpose.

3. **Data minimisation:** Personal data collected and used shall be limited to what is adequate, relevant, and not excessive in relation to a specific and defined purpose.

4. **Accuracy:** Personal data shall be accurate and, where necessary, kept up to date. Users shall have the right to erase, rectify, and correct their personal information.

5. **Retention limitation:** Personal data processed for any purpose shall not be kept for longer than is necessary.

6. **Users' rights:** Personal data shall be processed in accordance with the rights of users such as the right to access or right to erasure (See point 4).

7. **Integrity and confidentiality:** Personal data shall be processed in a manner that ensures state-of-the-art security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

8. **Adequacy:** Personal data shall not be transferred to a third country or territory, unless that country or territory ensures an adequate level of protection for the rights and freedoms of users in relation to the processing of personal data. Data protection frameworks shall provide for mechanisms enabling the free flow of data between countries while safeguarding a high level of data protection.

**Experience from the GDPR negotiations**

The eight data protection principles come largely from international standards, in particular the Convention 108 and the OECD guidelines.[18] These data protection principles are considered "as minimum standards" for the protection of fundamental rights by countries that have ratified international data protection frameworks. These principles should be the basis of any data protection framework and are present in a large number of data protection laws around the world, from the EU Data Protection Directive from 1995, the GDPR, and most data protection laws that are in place in Latin America.

[17] See UK Information Commissioner's Office, Data Protection Principles https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/
[18] Organisation for Economic Cooperation and Development, September 1980. Guidelines governing the protection of privacy and transborder flows of personal data. https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/OECD_Privacy_Guidelines_1980.pdf

## 3 DEFINE LEGAL BASIS AUTHORISING DATA TO BE PROCESSED

Any data protection law must clearly define the legal basis under which users' personal data can be processed. Any entity, public or private, seeking to process personal data must abide by at least one of the legal bases provided for in the law. These usually include the execution of a contract, compliance with a legal obligation, and a user's consent.

Consent shall be defined as an active, informed, and explicit request from the user. It must be freely given and the user must have the capacity to withdraw consent at any time. This means, for instance, that pre-ticked boxes would not qualify as valid consent. In addition, companies cannot deny a user access to a service for refusing to share more data than strictly necessary for the functionality thereof. Otherwise, consent would not be freely given.

**Experience from the GDPR negotiations**

The GDPR allows for six bases for processing personal data from contract to consent. [19] The definition of consent was strengthened and clarified during the negotiations compared to the definition provided for in its predecessor, Directive 95/46. The GDPR indicates that consent must be "a clear affirmative act establishing a freely given, specific, informed, and unambiguous indication" of the user. However, the GDPR also authorises the processing of data for so-called "legitimate interest" purposes defined by the entity using the information. This provision greatly limits users' control over their personal information as they are often unaware of any data collection or processing when entities rely on legitimate interest (see more on legitimate interest in point two of the "Don'ts" section).



## 4 INCLUDE A LIST OF BINDING USERS' RIGHTS IN THE LAW

Protecting users' data protection and guaranteeing their control over their personal information requires establishing a series of binding rights to exercise:

1. **Right to access** enables users to obtain confirmation from services and companies as to whether personal data concerning them have been collected and are being processed. If that is the case, users shall have access to the data, the purpose for the processing, by whom it was processed, and more.
2. **Right to object** enables users to say "no" to the processing of their personal information, when they have not given their consent to the processing of their data nor signed a contract. This right to object applies to automated decision-making mechanisms, including profiling, as users have the right not to be subjected to the use of these techniques.
3. **Right to erasure** allows users to request the deletion of all personal data related to them when they leave a service or application.
4. **Right to rectification** allows users to request the modification of inaccurate information about them.
5. **Right to information** ensures that users receive clear and understandable information from entities processing their personal data, whether these entities have collected this information directly or received it through third parties. All the information provided to the user shall be provided in concise, intelligible, and easily accessible form, using clear and plain language. This information shall include details about data being processed, the purpose of this processing, and the length of storage, if applicable. The entities shall provide their contact details and an email address to allow users to contact them in case there are issues.
6. **Right to explanation** empowers users to obtain information about the logic involved in any automatic personal data processing and the consequences of such processing. This right is crucial to bring accountability and transparency in the use of algorithms to make decisions that impact users' lives.
7. **Right to portability** enables users to move certain personal data they have provided from one platform to another offering similar services. To facilitate this process, interoperability between services shall be encouraged.

[19] See Article 6. European Union, Regulation 2016/679/EU 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) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Although this list is not exhaustive, these rights must be provided for by law, and not left to the discretion of entities using the data. Users shall be able to exercise any of these rights free of charge.

**Experience from the GDPR negotiations**

The GDPR provides users with all mentioned rights, free of charge. The provisions enshrining those rights set detailed obligations on entities processing data to implement, provide for, protect, and respect these rights.[20]

The GDPR is an important step in ensuring that users can freely exercise their right to data protection. However, to ensure that all measures will be effective, there should be further effort to raise awareness about the existence of the law and its content. Governments, public authorities, companies, and NGOs should work jointly to achieve that goal.

Finally, the exercise of certain rights such as the right to portability and the right to explanation are particularly relevant in the era of Big Data and artificial intelligence. However, the full realisation of these rights will not take place without the cooperation of private entities developing algorithms, products, and services. We must ensure that engineers will create the necessary tools to enable the execution and enjoyment of these rights. For instance, a right to portability means nothing if platforms are not interoperable.[21] Similarly, a right to explanation can only exist if employees of companies relying on algorithms fully understand their functioning, and if they know why an algorithm is being used, what data are used in the algorithm, what data are created by the algorithm, and what variables the algorithm uses to make a decision. Given the limited language of the GDPR on that right, several academics are putting into question even the legal existence and the feasibility of such a right.[22] It seems clear that the GDPR intended to create such an avenue for users but it will be necessary to get further guidance from data protection authorities and stakeholders on how to interpret the text in practice. In short, creating such rights is positive but the conditions for the exercise of those rights must also be developed.



## 5 DEFINE A CLEAR SCOPE OF APPLICATION

The rights and principles established in a data protection law ensuring users' protection shall apply at all times. This means, for instance, that if an entity is offering a public or private service that involves the processing of data that targets users in the EU, users' rights encompassed under EU law shall apply.

In the digital age, it can be difficult for legislators to ensure sufficient protection of personal data and the rights of users without applying the principle of extraterritoriality. To understand the benefits of the extension of the jurisdictional scope of data protection, we need to look at the issue not from an "establishment" perspective (where is the entity located?) but from a user's perspective (where is the user and where is the user from?). The objective of human rights law, such as data protection frameworks, is first and foremost to protect individuals at all times. It is therefore logical to ensure that users' rights are respected no matter where the entities using people's data are located.

[20] See Chapter 3. European Union, Regulation 2016/679/EU 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) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
[21] Article 29 Working Party on Data Protection, Guidelines on data portability. http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf
[22] Sandra Wachter, Brent Mittelstadt and Luciano Floridi, University of Oxford, Oxford Internet Institute. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469

Such application of the territorial scope also has the potential to raise the level of protection for users globally if companies and authorities start implementing data protection and privacy measures in their daily practices worldwide. In terms of competition, such jurisdictional measures can avoid a race to the bottom in terms of protection, whereby certain industries would decide to relocate their companies outside a country to avoid applying user-protective measures.

It is important to note however that extending the jurisdictional scope of a piece of legislation is not without risk and should be carefully considered by lawmakers. Conflicts of laws could arise and certain states could seek to extend the scope of rights-harming measures outside their borders using the same justification. Furthermore, not every entity processing data around the world knows about every country-specific law. It is often unclear whose obligation it is to inform businesses and individuals about their respective obligations and rights. Awareness-raising campaigns shall be conducted to ensure that entities around the world know their obligations. In order for data protection laws to properly function, public authorities need the mandate and resources to carry out public education. Civil society can and should have an active role in the process, in particular to empower people to enforce their rights.

Extending the scope of jurisdiction is not a one-size-fits-all solution and specific criteria should be established in data protection laws to limit bad copies or harmful consequences. Lawmakers should for instance clearly indicate under which scenarios the law applies outside their borders, to which actors specifically, what enforcement mechanisms will be in place, and provide users, companies, and authorities with clear avenues for remedies.

Finally, obligations under data protection law shall clearly apply to both the private and public sector. Public authorities are increasingly collecting individuals' information, getting access to private-sector databases, or otherwise building large databases of personal data. This processing shall be subject to clear obligations for the protection of individuals' personal information, the same way that processing by private entities is regulated.

**Experience from the GDPR negotiations**

The GDPR extends the territorial scope of the law compared to the 1995 Data Protection Directive. The GDPR applies to any companies and authorities established in the EU but also to entities established outside the EU if those are either processing personal information in connection with the offering of goods or services to, or monitoring of behaviour of, users who are in the European Union.[23] This important change in the scope of application of the law reflects the evolution of EU jurisprudence. For many years, courts in the EU battled with large tech companies that refused to comply with local data protection laws, based on issues of jurisdiction. Google and Facebook have repeatedly argued that they are not covered by data protection laws, for example, in Spain or Belgium, as they were not formally established in these countries. They took this position despite the fact that the companies were mining and monetising personal information from users in these countries.[24] [25] By extending the territorial scope of application, the GDPR sought to respond to these loopholes in protection for users and achieve legal certainty for users. This change is not however without challenges as it is not clear how EU data protection authorities will be able to conduct enforcement actions toward entities located outside the EU and therefore adequately protect rights.

[23] See Article 3. European Union, Regulation 2016/679/EU 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) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[24] Court of Justice of the European Union, Judgement in Case C-131/12, Google Spain SL vs Mario Costeja González, 13 May 2014. http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5eb572d024de249578524881c67efe5ec.e34KaxiLc3eQc40Lax-qMbN4PaN0Te0?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=-first&part=1&cid=574499

[25] Reuters, Facebook wins privacy case against Belgian data protection authority, June 2016. https://www.reuters.com/article/us-facebook-belgium-idUSKCN0ZF1VV

## 6 CREATE BINDING AND TRANSPARENT MECHANISMS FOR SECURE DATA TRANSFER TO THIRD COUNTRIES

Data protection frameworks are designed to ensure the free flow of data by establishing adequate mechanisms for data transfer and effective safeguards for users' rights. These mechanisms must be put under strict and transparent oversight and include effective remedies to ensure that the rights of users travel with the data.

### Experience from the GDPR negotiations

Under the GDPR, cross-border data transfer outside the European Economic Area may only take place if the transfer is made to a country that has been accorded an adequacy status or when a lawful data transfer mechanism is in place.[26] The GDPR provides for more mechanisms for transfer than the Directive from 1995 through codes of conduct and certification schemes. This approach provides companies with greater flexibility. Effective oversight and enforcement of these mechanisms will be crucial to ensure that users' rights remain protected during and after transfer.

Regarding adequacy, the European Commission has the power to determine whether a third country ensures an adequate level of protection by reason of its domestic law or due to the international commitments into which it has entered, thereby permitting data to be exported to that jurisdiction. Any country can apply for an adequacy decision which will launch a review process conducted at the sole discretion of the EU Commission. Currently, the European Union has granted adequacy to the following countries[27]: Andorra, Argentina, Canada, Switzerland, Faroe Island, Guernsey, State of Israel, Isle of Man, Jersey, New Zealand, United States of America, and Eastern Republic of Uruguay. Adhesion to the Council of Europe Convention 108 is of particular importance in that respect, and is one of the elements taken into consideration in the assessment of the adequacy granting.

In 2016, the US lost the arrangement called Safe Harbour on which its adequacy determination was based due to non-compliance with EU fundamental rights law.[28] The validity of several elements of its new arrangement (EU-US Privacy Shield) continues to be under scrutiny.[29] Other countries like Australia have been requesting an adequacy decision but have so far failed to meet the necessary requirements.[30] Finally, ongoing negotiations for review and new adequacy are currently taking place with Japan.[31]

[26] See Chapter 5. European Union, Regulation 2016/679/EU 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) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
[27] EU Commission, Commission decisions on the adequacy of the protection of personal data in third countries http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
[28] Access Now, CJEU declares Safe Harbor invalid https://www.accessnow.org/cjeu-declares-safe-harbour-invalid/
[29] Access Now, Comments to EU Commission on Privacy Shield review https://www.accessnow.org/cms/assets/uploads/2017/07/AN-PSReviewResponse-1.pdf
[30] European Commission, DG Justice, Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments http://ec.europa.eu/justice/data-protection/document/studies/files/new_privacy_challenges/final_report_country_report_b2_australia.pdf
[31] European Commission, Joint statement by Vice-President Andrus Ansip and Commissioner Věra Jourová on the dialogue on data protection and data flows with Japan, March 2017. http://europa.eu/rapid/press-release_STATEMENT-17-690_en.htm

## 7 PROTECT DATA SECURITY AND DATA INTEGRITY

To experience the benefits of the digital economy, users need to be able to trust the services they use online. Any data that are shared generates a risk. Therefore, it is increasingly important to ensure that privacy and data protection are considered by engineers in the design phase of product and services and that they are set to the highest standards of protection by default; this is the concept of data protection by design and by default. Those concepts should be spelt out in the law to require entities to adopt them.

**Experience from the GDPR negotiations**

The GDPR codifies the principles of data protection by design and by default which provides a large number of benefits, such as contributing to data security and integrity.[32] With privacy and data protection by design and by default, companies take a positive approach to protecting users' rights, by embedding privacy-protecting principles into both technology and organisational policy. Privacy and data protection becomes part of the company culture and accountability framework, rather than being a "simple" compliance element. This requires thinking about privacy and data protection from the beginning of the process of developing a product or service.[33] This approach can help companies save on development costs for products or services. Because engineers and development teams will have considered privacy and data protection at the outset of the development phase, there would be fewer adjustments that would have to be made when a legal team reviews the final product. It also reduces the risk of a company being sued for privacy violations or suffering reputational damage due to data leaks, as it would be able to demonstrate its commitment to users' rights. In short, moving from understanding privacy and data protection as a compliance issue to embedding privacy and data security by design and by default can help companies increase trust in their services.

## 8 DEVELOP DATA BREACH PREVENTION AND NOTIFICATION MECHANISMS

While data protection frameworks should encourage measures fostering data security and data integrity, data breaches can still take place. Measures to address, remedy, and notify users of such problems shall therefore be put in place. Data breaches have gained widespread attention as businesses of all sizes become increasingly reliant on cloud computing and online services. With personal and sensitive data stored on local devices and on cloud servers, breaching network and information security has become attractive to those seeking to expose or exploit private information or demand a ransom. Data breaches have existed for as long as individuals' private records have been maintained and stored. Before the digital era, a data breach could be something as simple as viewing an individual's file without authorisation, or finding documents that weren't properly disposed of.[34] With the digitisation of records and ever-growing personal data collection, the scale of data breaches has skyrocketed, putting users' personal information at greater risk.

[32] See Article 25. European Union, Regulation 2016/679/EU 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) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
[33] For more information on Privacy by Design see Ann Cavoukian, Privacy by Design, the 7 Foundational Principles https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf
[34] Nate Lord, The history of data breaches, July 2017. https://digitalguardian.com/blog/history-data-breaches

To prevent and mitigate these risks, mechanisms for data breach notification and prevention of such breaches should therefore be developed, either within a data protection framework or in complementary legislation. High-profile incidents of personal data loss or theft across the globe have prompted wide debate on the level of security given to personal information shared, processed, stored, and transmitted electronically. In that context, gaining and maintaining the trust of users that their data are secure and protected represents a key challenge for organisations. The NGO Privacy Rights Clearinghouse have recorded 7,619 data breaches that have been made public since 2005 in the US alone.[35] This means that at least 926,686,928 private records have been breached in the US since then. IBM and Ponemon Institute report that in 2017 the global average cost of a data breach is $3.62 million.[36] While this cost has slightly decreased compared to last year, the study shows that companies are having larger breaches. Other studies estimate that the average cost of a data breach will be over $150 million by 2020, with the global annual cost forecast to be $2.1 trillion.[37] This means that preventing and mitigating data breaches is not only good for users, but also good for businesses in order to save costs.

## Experience from the GDPR negotiations

Data breach notification requirements were introduced in the European Union for the electronic communication sector in 2002.[38] Further specific sectoral rules have been developed since then to serve until those measures are harmonised under the GDPR to facilitate compliance for organisations.

The measures adopted under the GDPR require an organisation to report a data breach "without undue delay" and where feasible within 72 hours after it becomes aware of the incident.[39] While it is clear that the objective of the measure is to ensure that data breaches are reported as quickly as possible, the language is vague. The GDPR then describes the steps that any organisation encountering a breach must follow and provides for the possibility of notifying users. Such notifications are positive from an accountability and transparency perspective and are also crucial to ensure that users can take appropriate action to secure their information and seek remedy if necessary. However, the GDPR leaves it up to organisations to determine whether to notify users of a breach based on their own risk assessment of users' rights and freedoms. Notification to users should be a requirement for any data breach of personal data, which includes not only subscriber information, but other personal data such as photos. Notification should be timely, easy to understand, and comprehensive, and remediation options should be clearly indicated and accessible. By leaving too much discretion to organisations, this provision falls short of empowering users to take control of their information. Organisations suffering a data breach have an obvious economic interest in downplaying the risks associated with a breach and not notifying users, which could result in unaddressed data protection violations. We encourage lawmakers around the world to avoid those shortcomings and develop unambiguous data breach prevention and notification mechanisms.



[35] Privacy Rights Clearinghouse, Data Breaches. https://www.privacyrights.org/data-breaches
[36] Ponemon Institute for IBM, 2017 Cost of Data Breach Study: Global Overview https://www.ibm.com/security/data-breach/
[37] The Experian, Data Breach Industry Forecast, 2015. https://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf
[38] European Union, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML
[39] See Articles 33 and 34. European Union, Regulation 2016/679/EU 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) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

## 9 ESTABLISH INDEPENDENT AUTHORITY AND ROBUST MECHANISMS FOR ENFORCEMENT

No data protection framework can be complete without a robust enforcement mechanism which includes the creation of an independent supervisory authority (data protection authority — DPA — or commission). Even the best data protection law in the world would be close to meaningless without an authority having the powers and resources to monitor implementation, conduct investigations, and sanction entities in case of (repeated, neglected, or willful) data protection violations.

Sanctions should be proportionate to the violations and can be in the form of notice to action. Authorities can for instance request a company stop certain practices that violate users' rights to data protection, such as the failure to provide a privacy policy or selling users' sensitive information without their knowledge and consent.

While punitive fines need to exist, data protection authorities shall apply limited fines to companies, in particular small or medium enterprises (SMEs), that do not engage in significant data processing, do not have the means to understand their obligations to respect data protection law, and have made mistakes out of ignorance rather than malice. Government shall also conduct awareness-raising efforts in order to avoid situations where companies would be ignorant of the existence and relevance of data protection laws. Tunisia, which is currently discussing its first ever data protection law, is proposing a quite innovative gradual approach to sanctions which includes higher fines in cases of recidivism.[40] As a result, a company found to commit data protection violations for which it has already been sanctioned would receive a significantly higher fine.

Sanctions and fines however represent only a small part of the work of DPAs. The role of data protection authorities is of course to enforce data protection laws and conduct oversight but also to assist organisations in their compliance duties. This means that companies, public authorities, and NGOs shall cooperate with data protection authorities to understand each other's duties and obligations. Organisations should not hesitate to establish contact with their DPA which can provide them with resources and materials to help implement the law.

Finally, DPAs have the powers to launch independent investigations into organisations and to hear cases brought to them by individuals or NGOs. In that sense, DPAs act as a guardian for users' rights and can help protect fundamental rights. These authorities are however still largely unknown by users around the world. To further help protect users' rights, NGOs should be empowered to represent users and to independently bring cases in front of DPAs and courts. Governments shall also further promote the work of DPAs, explain their role, and provide them with an adequate budget to ensure that DPAs can fulfil their duties.

**Experience from the GDPR negotiations**

The European Union and its member states have had data protection laws for almost 30 years. Despite this, many companies were ignoring them due to the lack of enforcement powers for data protection authorities and the relatively low level of fines (up to 150.000€).[41] For years in Europe, legal advisers often advised companies not to comply with EU data protection law, as the risk of being fined was as low as the amount they would have to pay.[42] This blatant disregard for fundamental rights was addressed under the GDPR by raising the fine level to a maximum of 4% of the worldwide turnover of the company.[43] The enforcement powers and the functioning of the DPAs have also been clarified and harmonised. DPAs will now be gathered within a European Data Protection Board which allows them to, for instance, conduct joint investigations across different EU countries.

[40] Tunisia national authority for the protection of personal data. Article 211. Projet de loi relative à la protection des données personnelles, 2017. http://www.inpdp.nat.tn/Projet_PDP_2017.pdf
[41] European Union. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046
[42] See Panel discussion at Computer, Privacy and Data Protection, Brussels, 2015. https://www.youtube.com/watch?v=sikwHfoiylg
[43] See Chapters 7 and 8. European Union, Regulation 2016/679/EU 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) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

## 10 CONTINUE PROTECTING DATA PROTECTION AND PRIVACY

Having a comprehensive law is a great milestone, but it does not mean governments should stop here in the protection of personal data and privacy. New challenges to privacy and data protection are likely to emerge during implementation phases even if governments aim at making laws "future-proof." This means that a review process will likely be necessary, which is a great opportunity to update the law, address any potential issues with compliance, and provide additional clarity and legal certainty where needed.

It is also important to understand a data protection law as a floor and not a ceiling in the protection of users' rights. This means that organisations must comply with the law, as a minimum, but should also be encouraged to go beyond and take further actions to protect people's privacy. Similarly, depending on the structure and form of the government of a country, different approaches to data protection and privacy can be taken into account. For instance, in the US, the federal government should not prevent local governments and states from providing for user protections, in addition to the limited measures provided at the federal level, and refrain from using its power to preempt regional and local laws.[44] However, in the case of the European Union, member states shall avoid creating additional rules as this would risk fragmenting the harmonised high level of protection for users agreed under the GDPR.

### Experience from the GDPR negotiations

Since 1995, EU member states have adopted different local data protection laws based on the benchmark provided by the EU Data Protection Directive. This EU law was completed at a time when only 1% of the population was online, and it was in urgent need of modernisation when the EU Commission proposed the EU General Data Protection Regulation in 2012.[45] It took almost five years of negotiations for lawmakers to agree to the new measures in the law which will become directly applicable from May 2018 (unlike a Directive, which needs to be transposed into national law, a Regulation is directly enforceable). All 28 national data protection laws will be replaced by this single law that provides for harmonised rights and rules across the EU. While this system works under the EU's legal order, it might not be the ideal scenario in other regions or countries. Supranational laws can be difficult to agree upon and might not necessarily be the best instrument to protect users. There is therefore no ideal model for a law but all data protection laws shall take into account all the points laid down in this paper.



[44] EPIC, Privacy preemption watch. https://epic.org/privacy/preemption/
[45] European Commission, Reform of EU data protection rules, 2012. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

# DON'TS

Below you will find five recommendations for policy makers to follow when developing a data protection law. We advise caution on the following five elements which, if ignored, could limit the benefits of the proposed law or harm individuals' rights.

## 1 DO NOT SEEK BROAD DATA PROTECTION AND PRIVACY LIMITATIONS FOR NATIONAL SECURITY

Governments not only have an obligation but also a security interest in ensuring the protection of personal data, in particular when information is held by government agencies. In 2015, as the result of a cybersecurity incident in the US, 21.5 million records of federal employees and family members stored at the Office of Personnel Management were stolen.[46] As these types of incidents and attacks are increasing globally, countries have must take measures to better protect individuals' information.

Despite this, governments often seek limitations to data protection and privacy rights for their own use of personal data by asking for broad exceptions. These exceptions must be prevented and limited to clearly defined, necessary, and proportionate measures that include judicial oversight and accessible remedy mechanisms. Legislation should not give governments and public entities the capacity to shield themselves from the obligation to protect users' right to data protection. Countries have a security interest in safeguarding personal data held by government agencies.

**Experience from the GDPR negotiations**

The GDPR provides a list of reasons that member states can rely on to restrict users' rights and freedoms protected under the law, such as national security or defence.[47] While it is common to find provisions allowing states to restrict rights in every piece of EU and national legislation, the language of these provisions is often purposefully vague and can potentially cover a wide range of state activities. The GDPR for instance allows for restrictions of rights for broad and undefined "other important objectives of general public interest of the Union or of a Member State". Given the impact of such restrictions on users' rights and freedoms, they should be clearly defined and limited in law, subjected to strict transparency and oversight criteria, and be necessary and proportionate measures in a democratic society.

## 2 DO NOT AUTHORISE PROCESSING OF PERSONAL DATA BASED ON THE LEGITIMATE INTEREST OF COMPANIES WITHOUT STRICT LIMITATIONS

Companies often argue that they should have a right to collect and process user data, when this is their "legitimate interest", without having to notify users. Unless such exceptions are defined as being exceptions (not the case under the GDPR or the 1995 Directive) and narrowly defined (which is better achieved in the GDPR), this should not be allowed. Otherwise, this intrinsically contradicts the objective of data protection, which is to put users in control of their information. Such attempts to limit users' rights must be prevented.

[46] Patricia Zengerle, Megan Cassella, Millions more Americans hit by government personnel data hack, Reuters, 2015. https://www.reuters.com/article/us-cybersecurity-usa/millions-more-americans-hit-by-government-personnel-data-hack-idUSKCN0PJ2M420150709
[47] See Article 23. European Union, Regulation 2016/679/EU 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)

**Experience from the GDPR negotiations**

Organisations' legitimate interest is one of the legal bases that can be used to process personal data under the GDPR.[48] The core of data protection is users' control and predictability in the use of their data. The legitimate interest provision goes against these principles. Under "legitimate interest" an organisation is authorised to collect and use personal information without having to notify the concerned users. If you don't know that an entity holds data about you, how could you exercise your right to access the data or your right to object?

This provision was one of the most debated during the negotiations of the GDPR. Companies were defending a broad and vaguely defined provision for legitimate interest and civil society was trying to remove it or significantly limit its scope. Lawmakers tried to limit the impact of the provision in the last months of negotiations by including a requirement for companies to balance their legitimate interest with fundamental rights. While the intention is laudable, companies will conduct this assessment at their own discretion and users could be kept in the dark. The final result is satisfying for no one as businesses wanted even more flexibility than accorded in the text and corresponding recitals, and NGOs wanted clear limitations. We understand the need to provide companies with measures that allow them to conduct business, however, measures that prevent users from having control over their personal information shall be excluded as they contradict the spirit and objective of a data protection law.



## 3 DO NOT DEVELOP A "RIGHT TO BE FORGOTTEN"

The "right to be forgotten" or "right to de-list" emerges from EU data protection law including the "Google Spain" ruling.[49] This right allows users under certain circumstances to request search engines to de-list web addresses from results when a search is done using their names. This right should not be confused with the right to erasure which allows individuals to delete all personal data related to them when they leave a service or application. The right to erasure is essential to ensure user control over personal information. It also should not be conflated with any take-down measure since the right to be forgotten developed under EU jurisprudence does not require or request any online content to be removed from the web or from search engine indexes.

The way several governments internationally have, accidentally or otherwise, misinterpreted the right to de-list or sought to extend its scope to limit freedom of expression or of information poses a significant threat to human rights. Courts and legislators around the world have demonstrated significant interest in developing measures to establish a "right to be forgotten" which significantly deviates from the approach developed by EU

[48] See Article 6. 1. (f). European Union, Regulation 2016/679/EU 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) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[49] Court of Justice of the European Union, Judgement in Case C-C-131/12, Google Spain SL vs Mario Costeja González, 13 May 2014. http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5eb572d024de249578524881c67efe5ec.e34KaxiLc3eQc40Lax-qMbN4PaN0Te0?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=-first&part=1&cid=574499

courts, mandating content removal.[50] [51] [52] Any so-called right to be forgotten measure that would lead to deletion of online content is a gross misinterpretation of the right. Under no circumstances must the right to de-list be applied to enable the removal of online content. Similarly, data protection authorities shall not be authorised to request the deletion of online information without the oversight of a judge that can ensure that all fundamental rights, including the right to free expression and freedom to access information, are respected.

Access Now opposes any development of such a "right to be forgotten". If however a right to de-list similar to the one in place in the EU were to be considered by lawmakers, Access Now has identified a series of legal safeguards that lawmakers must put in place to further mitigate the risks of abuse and harms to human rights.[53]

**Experience from the GDPR negotiations**

The right to be forgotten was added to the right to erasure in the GDPR.[54] The right to be forgotten codifies the jurisprudence of the EU Court of Justice in the "Google Spain" case.[55] The court has developed a set of criteria for search engines to consider when they receive a de-listing request. Search engines must grant a de-listing request only if the personal information included in the designated web address is "inadequate, irrelevant, or no longer relevant, or excessive", and only if the information does not pertain to a public figure or is not of public interest. However, information or links shall not be removed from the search index. They must remain accessible when users conduct searches using terms other than the name of the individual making the de-listing request. Importantly, the GDPR also clarifies that information shall not be de-listed if it is necessary for exercising the right of freedom of expression and information.

Despite those safeguards, further guidance from the EU and its member states is necessary to ensure that search engines do not "over- or under-comply" with the law and the ruling. Uncertainty regarding the geographical scope of application of the right to be forgotten has for instance led to new legal proceedings.[56] For their part, search engines should be more transparent about the criteria they have been using internally to deal with these requests.

Finally, in the current implementation of the right to de-list in the EU, access to remedy is limited. The only form of recourse that a user has is the opportunity to challenge a search engine's decision to deny a request to de-list. There should be more clarity on existing avenues for remedy, and these should be extended.



[50] Access Now, O direito ao esquecimento no Brasil: quais os riscos para os direitos humanos? https://www.accessnow.org/o-direito-ao-esquecimento-no-brasil-quais-os-riscos-para-os-direitos-humanos/
[51] Access Now, Documento de posición: El "derecho al olvido" y su impacto en la protección de los Derechos Humanos https://www.accessnow.org/documento-de-posicion-el-derecho-al-olvido-y-su-impacto-en-la-proteccion-de-los-derechos-humanos/
[52] Access Now, In India, the "right to be forgotten" is in the hands of the Delhi High Court https://www.accessnow.org/india-right-forgotten-hands-delhi-high-court/
[53] Access Now, Understanding the right to be forgotten globally, September 2016 https://www.accessnow.org/cms/assets/uploads/2016/09/Access-Not-paper-the-Right-to-be-forgotten.pdf
[54] See Article 17. European Union, Regulation 2016/679/EU 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) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
[55] Access Now, FAQ on the right to be forgotten, 2014. https://www.accessnow.org/cms/assets/uploads/archive/docs/GoogleSpainFAQRtbF.pdf
[56] Access Now, Only a year until the GDPR becomes applicable: Is Europe ready? https://www.accessnow.org/year-gdpr-becomes-applicable-europe-ready/

## 4 DO NOT AUTHORISE COMPANIES TO GATHER SENSITIVE DATA WITHOUT CONSENT

Given the importance of sensitive data, a higher level of protection than for the rest of personal data must be required to guarantee an adequate level of control for individuals. Therefore, the collection and processing of sensitive personal data shall only be authorised if individuals have given their explicit, informed consent and have the right to withdraw that consent subsequently.

Sensitive data encompasses a wide range of personal information such as ethnic or racial origin, political opinion, religious or other similar beliefs, memberships, physical or mental health details, such as genetic or biometric data, information about personal life and sexuality, or criminal or civil offences. The particular nature and relevance of this information means that users should always be able to control who gets access to and use of this information. As a result, the processing of sensitive information should only be authorised if users have freely given informed and explicit consent. To protect the essence of users' fundamental rights to privacy and data protection, no exception to these rules shall be allowed.

**Experience from the GDPR negotiations**

The GDPR requires organisations to obtain the explicit consent of the user for the collection of sensitive data as a general basis. While this is extremely positive, the law also authorises the collection and use of sensitive data without users' consent for some specific objectives, including "scientific or historical research purposes or statistical purposes".[57] This broad exception deprives users of control over their most intimate information and is even more problematic in the context of the growth of the e-health industry, large scale, Big Data analysis of political views, and more. If not limited, companies could get a hold of millions of pieces of sensitive information over the next few years, initially to conduct research and gather statistics on their products. In practice, it would be complex to conduct oversight of how organisations use these data, as users will not be informed. Users must be able to control which organisation has access to their health or voting records. This type of loophole must be avoided, or at least strictly limited by restricting the use of these data for research, and statistical research must be conducted in the public interest under strict oversight.

## 5 DO NOT FAVOR SELF-REGULATION AND CO-REGULATION MECHANISMS

For many years, companies and entities collecting data have been calling for regulation of privacy and data protection not through binding frameworks but rather through self- or co-regulation mechanisms that offer greater flexibility. Despite several attempts, there are no examples of successful non-binding regimes for the protection of personal data or privacy that have been positive for users' rights or, indeed, business as a whole.

As more data are being shared online and off, it is high time to develop mandatory frameworks for data protection and privacy all around the world to prevent or end these behaviours and put users back in control of their information. This will also enable the development of privacy-friendly innovation which is currently limited to a small number of companies that have undertaken a long-term engagement approach to protect their users instead of basing their business model in monetising users' private information.

[57] See Article 9.2.(j). European Union, Regulation 2016/679/EU 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) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Business models built on privacy can serve as a competitive advantage. In countries without overarching data protection laws, companies could innovate through their internal practices by developing voluntary safeguards and guidelines to improve people's trust in the digital economy. Even though self-regulation is inadequate as an enforcement mechanism and unsustainable for safeguarding individuals' rights, it can be beneficial in certain circumstances for both companies and individuals to adopt a voluntary framework in those countries. It cannot be relied upon, either from the perspective of individuals or businesses, due to the risk of "free-riding" by bad actors that will undermine privacy, trust, innovation and take-up of new products.

**Experience from the GDPR negotiations**

The European Union has a long experience of failed self- or co-regulation attempts in the area of free expression.[58] In the field of privacy and data protection, however, the EU has been a pioneer in the development of a high-level of protection for users. The GDPR is yet another example of that success. While far from perfect, the GDPR is a key instrument for the protection of fundamental rights in the EU, and reflects years of experience gleaned from the implementation of past laws and jurisprudence developed by courts. The GDPR creates clear and strong obligations for organisations but also introduces several accountability tools to further data protection rights such as the principles of data protection by design and by default and new provisions for company certification and industry-wide code of conduct schemes. Such tools aim to develop a vision of data protection beyond mere compliance with the law and encourage innovation in the field.



[58] EDRi, Human rights and privatised enforcement https://edri.org/wp-content/uploads/2014/02/EDRi_HumanRights_and_PrivLaw_web.pdf

## CONCLUSION

Access Now wholeheartedly supports the development of local, regional, and international frameworks for the protection of personal data. These frameworks must be user-centric and focus on safeguarding and strengthening rights, while delivering clear and predictable rules for public and private entities to comply with. Last, but not least, we cannot highlight enough the importance of comprehensive and robust enforcement mechanisms overseen by an independent authority to ensure that the proposed protections are fully functional.

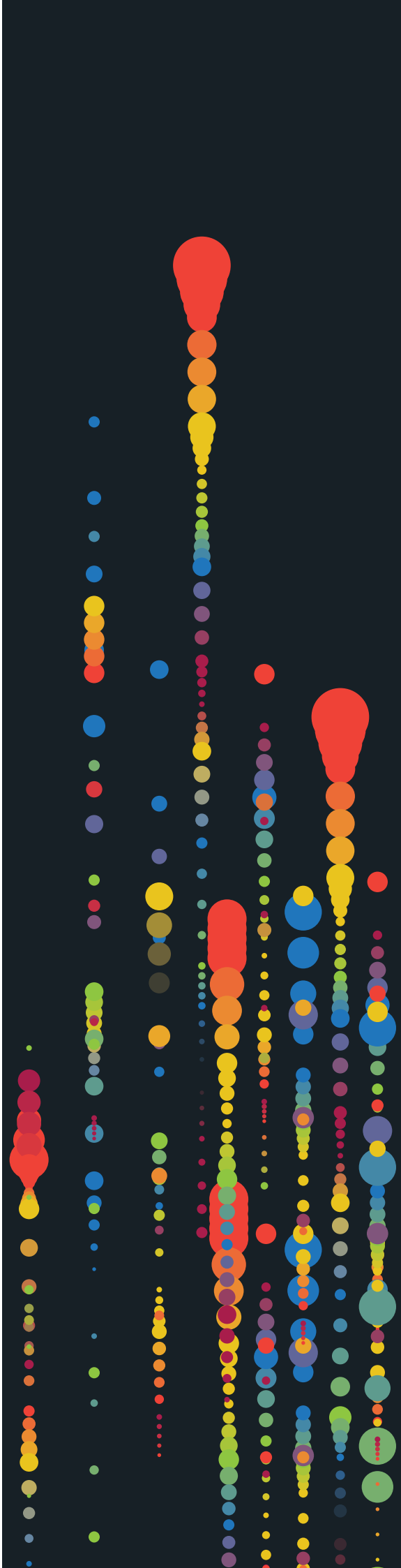
Protecting data protection globally has been a long-time area of focus for Access Now, and it continues to be one of our highest priorities. Among other issues, our team is actively engaged in the implementation of the GDPR, the reform of the data protection legislation in Argentina, and negotiations in India and Tunisia for developing a first data protection law.

**CREATING A DATA PROTECTION FRAMEWORK:**
**A DO'S AND DON'TS GUIDE FOR LAWMAKERS**

**November 2018**

**This paper is an Access Now publication.**

For more information, please visit: **https://www.accessnow.org,** or
contact: **Estelle Masse** | Senior Policy Analyst | **estelle@accesnow.org**



accessnow

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

**https://www.accessnow.org**