Data protection regulations around the world

The society in which we live as individuals and entrepreneurs is increasingly digitised. The use of digital tools and the internet has become highly accessible in many areas, bringing with it many changes and leading to new modes of consumption and interaction.

Much of our data is now digitised, stored in computer systems and put online. Data protection is therefore crucial if users are to be protected. To stay competitive, companies have been forced to integrate new technologies while complying with new legal frameworks. By now, the issue of data protection has become both a crucial and strategic one if companies are to stay sustainable and strengthen their reputation.

It is therefore essential that companies fully understand legal frameworks relating to data protection around the world to make sure they are complying with them. This guide is not exhaustive, but provides businesses with an overview of the different data protection regulations.

What is data protection and why should it be regulated?

Data protection laws protect individuals' fundamental rights and character. The main goal is to protect the person rather than the data itself. Data protection refers to the practice of securing and protecting personal, sensitive information belonging to individuals or organisations, preventing it from unauthorised access, use, disclosure and alteration. It aims to guarantee the confidentiality, integrity and availability of data, while respecting fundamental rights to privacy and data protection.

Do not confuse personal data with sensitive data

According to the Data Protection Act (DPA), personal data refers to any information relating to an identified or identifiable natural person.

Sensitive personal data includes data on religious, philosophical, political or trade union opinions or activities; data on health, personal sphere or racial or ethnic origin; genetic data ad biometric data unequivocally identifying a natural person; data on criminal and administrative proceedings or sanctions; and data relating to social services measures.

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0
All the contents of this document may be shared, copied, reproduced, distributed, communicated, reused and adapted by any means and in any format, provided that the author is mentioned (State of Geneva) and the same license is used for all related content (CC – BY – SA 4.0).

REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX
h e g Haute école de gestion Genève
UNIVERSITÉ DE GENÈVE

Learn more

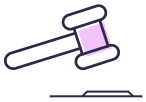
Issues with data protection

- **Individual rights**
  Guaranteeing individuals the right to control, access and correct their personal data.

- **Growing threat of breaches**
  With the rise of digital technology, risks of data breaches have increased; this includes data loss, destruction, alteration, disclosure and unauthorised access such as hacking.

- **Consumer trust**
  Strengthening the trust between businesses and their customers and partners, so that they know their data is being treated securely.

- **Corporate responsibility**
  Businesses have an obligation to adopt the appropriate security measures and be transparent about how they use data.



- **Sanctions**
  In the event of non-compliance, businesses and/or individuals may be subject to substantial fines, reinforcing the importance of compliance.

- **International standardisation**
  Regulation helps establish common standards for data protection across borders, facilitating international information exchanges.

The swiss federal data protection act

In Switzerland, the legislation for data protection is called the Federal Data Protection Act **(loi fédérale sur la protection des données / LPD)**, or **Datenschutzgesetz (DSG)** in German. The first LPD was established in 1992. With the dawn of the internet, the LPD had to be completely revised to ensure that the population had adequate protection over their data, adapted to recent technological developments. It was also essential to revise the law so that Swiss law continued to be compatible with European law, particularly **General Data Protection Regulation (GDPR)**. This guarantees the free movement of data with the European Union.

The new LPD came into force on 1 September 2023 with immediate effect, completely replacing the old law of 1992. The law aims to improve the way in which personal data is processed and grants Swiss citizens new rights; for companies, it also comes with a certain number of obligations.

The law's provisions for implementation, as enshrined in the new **ordinances on data protection (OPDo)** and **data protection certifications (OCPD)** came into effect at the same time as the DPA, on 1 September 2023.

The 7 principles of data protection

- Lawfulness, fairness, and transparency
- Data minimisation
- Storage limitation
- Purpose limitation
- Accuracy
- Integrity and confidentiality (security)

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

A brief history

24 June 1976
Adoption of the Automatic Computer Processed Information Act (ATIA)

19 June 1992
Swiss Federal Data Protection Act (LPD) comes into effect

25 May 2018
General Data Protection Regulation (GDPR) comes into effect

1 March 2019
Partial revision of the LPD

25 August 2023
European regulations Digital Services Act (DSA) and Digital Market Act (DMA) for large platforms come into effect

1 September 2023
New Federal Data Protection Act (LPD) comes into effect

17 February 2024
European regulations Digital Services Act (DSA) and Digital Market Act (DMA) for smaller platforms come into effect

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

Companies affected by data protection law

All companies active in Switzerland or carrying out business in Switzerland are affected, and are obliged to comply with the new data protection provisions immediately.

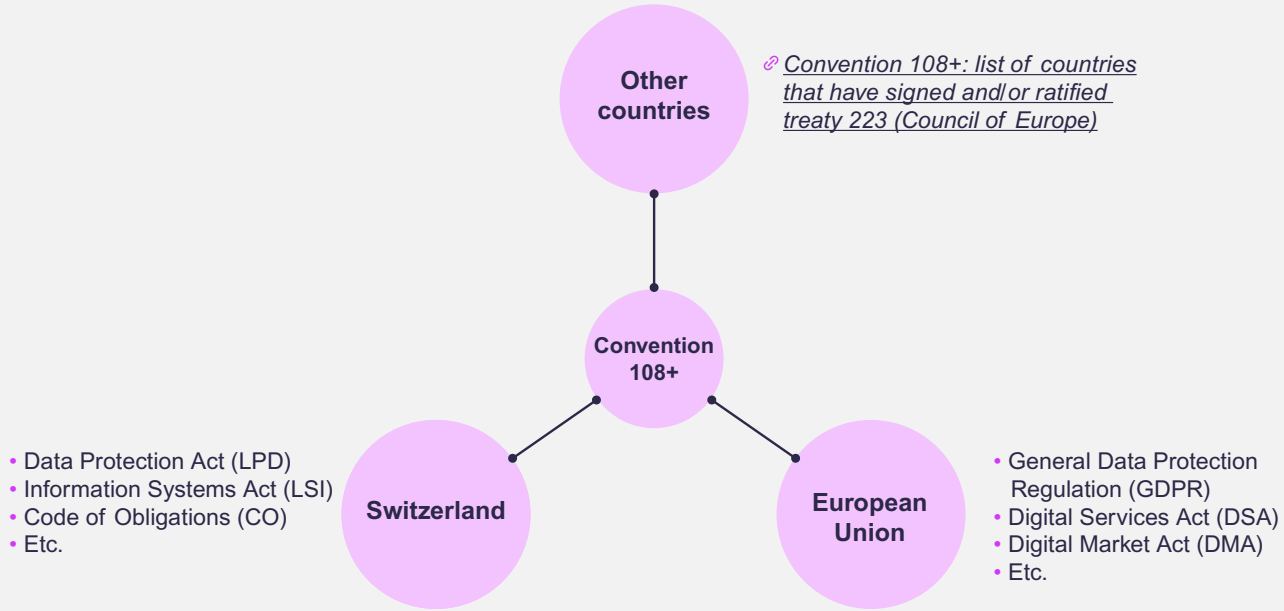
Switzerland and convention 108+

Although Switzerland is not a member of the European Union, it has signed Convention 108+, committing to adopt practices similar to those of other countries that have ratified the convention on the processing of personal data.

Convention 108+ is a treaty established by the Council of Europe and relates to the protection of individuals with regard to automatic processing of personal data. Its objective is to define data protection guidelines in order to ensure respect for individuals' rights and freedoms, particularly with regard to their privacy when their information is used.

Convention 108 was introduced in 1981 and was the first legally binding international instrument. In 2018, the treaty was updated and renamed Convention 108+. This update strengthens the rights of individuals and modernises the principles of data protection in the digital age, particularly through increased protection against risks linked to automatic processing.

Convention 108+ is open to states that are not members of the Council of Europe. It therefore has an impact beyond Europe.

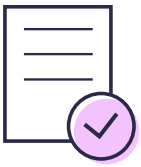


Convention 108+: list of countries that have signed and/or ratified treaty 223 (Council of Europe)

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

The need to respect regulatory frameworks regarding personal data protection

In most countries, data protection regulations are designed to safeguard the interests of both individuals and businesses against the harmful consequences of the unregulated use of personal information. These regulations not only govern the use of data to guarantee the rights of individuals; more broadly, they establish principles and good practices for collecting, processing and managing data. They thus ensure that companies and people required to process data maintain confidentiality and the secure and ethical use of information. In Switzerland, it should be noted that the LPD protects natural persons but not legal entities.



Compliance with data protection regulations is essential not only to avoid legal risks, but also to ensure the sustainable development and operation of the business. Digital confidence is a strategic issue for companies: it allows them to stand out on the market, maintain and develop the trust of their customers, and helps ensure prosperity.

Breaches can be expensive

Depending on the country, regulations and severity of the breach, fines can be substantial, from a few thousand francs to several million.

In Switzerland, natural persons can be sanctioned under the national Data Protection Act up to CHF 250,000. If no perpetrator with commensurate efforts can be found, the Act provides that companies are liable to pay a subsidiary fine up to a maximum of CHF 50,000.

Much harsher penalties are applied in the European Union, where financial sanctions can be up to 20 million euros or, for companies, up to 4% of the global annual turnover.

« The data protection law has new liabilities for companies, but it also promises to be a vector of new economic opportunities that are conducive to innovation and sector growth.»

Dessislava Leclère,
Lecturer at Geneva Business School

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

The need to respect regulatory frameworks regarding personal data protection

When business comply with regulations, they open up to many opportunities:

- Investing in data protection means investing in your business's cyber security. By allocating adequate resources to the security of data and information systems, companies strengthen their resistance against digital risks and threats.
- By guaranteeing the confidentiality, integrity and availability of data, companies strengthen and develop their reputation and trust with customers, partners and teams.
- Compliance protects companies from consequences that could lead to a loss of trust internally from employees, or externally from customers or partners, such as bad publicity and negative media coverage, difficulties recruiting, and a drop in attractiveness if the company is perceived as negligent when it comes to security, ethics and confidentiality.
- By complying with regulatory frameworks and anticipating risks related to data protection, companies can maintain access to the market and develop new markets. Compliance avoids the risk of being excluded from public procurement, which requires guaranteed compliance with data protection regulations and practices.
- Adopting a responsible, transparent approach towards stakeholders allows companies to promote their activities and values, and thus stand out from the competition.
- By implementing adequate digital risk management measures, companies avoid financial risks. Risks may include: potentially high fines, costs linked to repairing damage suffered by stakeholders, costs linked to implementing corrective measures after an incident, an increase in insurance premiums, a drop in the value of assets such as the customer database if it is stolen, etc.
- Various operational and technical risks may arise, leading to an interruption of all or part of the business, negative impact on the smooth running of the company, and an increase in the risks of cyber-attacks if preventive actions that meet the agreed standards are not implemented.
- When the regulatory frameworks in force are respected, companies avoid being exposed to legal and contractual risks, such as risks of legal action from customers, partners or even governments, as well as potential restrictions or prohibitions around processing certain kinds of data. Companies also take responsibility for subcontractors' proper compliance with the regulatory framework.

  They must therefore ensure the proper application of the laws both for themselves and for subcontractors.

Data protection officer

The cantonal Data Protection and Transparency Officer (PPDT) oversees the application of cantonal law on data protection and transparency.

In Geneva, this relates to the law on public information, access to documents and the protection of personal data (LIPAD), which applies to the Geneva public sector.

The Federal Data Protection and Transparency Officer (PFPDT) is responsible for overseeing the proper application of federal data protection provisions. In particular, the official monitors the way in which companies process data. It is also the mediation body for accessing official documents.

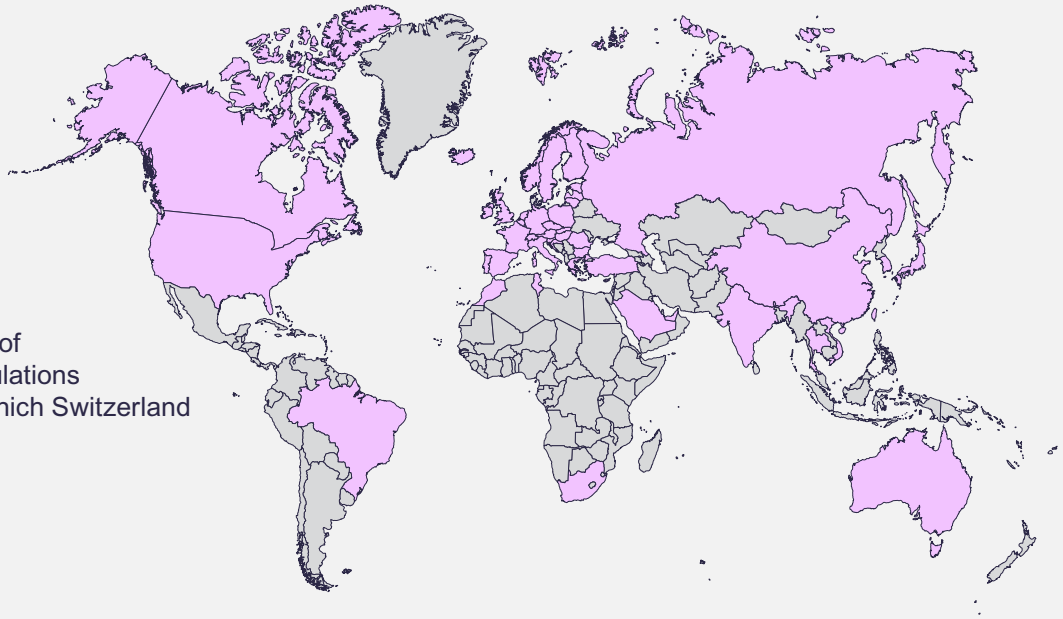
This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

Regulatory frameworks around the world

With so much data exchanged online every day, the need to preserve privacy and ensure data security is becoming increasingly important in many countries.

According to the United Nations Conference on Trade and Development (UNCTAD), at the end of 2021, 137 out of 194 countries had implemented direct or indirect regulations to protect data and privacy.

Non-exhaustive list of data protection regulations for countries with which Switzerland conducts business



Switzerland	Loi sur la protection des données (LPD) / Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG) / Nuova legge sulla protezione dei dati (LPD)	2023
European Un-ion	Règlement général sur la protection des données (RGPD)	2018
United King-dom	UK General Data Protection Regulation	2021
Norway	Personvernforordningen GDPR	2021
Iceland	Almenna persónuverndarreglugerði	2018
Türkiye	Kişisel verilerin korunmasi kanunu	2016
United States	Lois spécifiques par État	2020
Canada	Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)	2020
Brazil	Lei Geral de Proteção de Dados Pessoais	2020
Tunisia	Loi sur la protection des données à caractère personnel	2004
Morocco	Loi relative à la protection des données des personnes physiques à l'égard des traitements des données à caractère personnel	2009
South Africa	The Protection of Personal Information Act (POPIA)	2020
United Arab Emirates	القانون الاتحادي بشأن حماية البيانات الشخصية	2021
Russia	О персональных данных	2006
India	Information Technology Act	2020
China	Personal information protection law (PIPL)	2021
Hong Kong	Personal Data (Privacy) Ordinance	1996
Japan	個人情報の保護に関する法律	2017
South Korea	개인정보 보호법	2011
Taiwan	Personal Data Protection Act	2015
Singapore	Personal Data Protection Act	2012
Thailand	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล	2019
Vietnam	Nghị định bảo vệ dữ liệu cá nhân (Nghị định BVDLCN)	2023
Australia	Privacy Act	1988

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

Liabilities for various data protection regulations

States where an adequate level of data protection is guaranteed	**Assessment of the adequate level of protection including data transfers.** *Data Protection Ordinance (OPDo)*
Information obligation	All companies have an obligation to communicate clearly and trans-parently the purposes, sources and methods of processing personal data to the persons and/or entities concerned.
Activity log	Companies are required to maintain an up-to-date register of their activities, listing all personal data processing operations.
Impact analysis	Depending on the category of data processed by companies, an impact analysis must be carried out on the risks of processing per-sonal data to guarantee data protection.
Consent for processing sensitive data	Depending on the type of processing and data processed, com-panies must obtain explicit, informed consent from the persons whose data they are processing.
Notification of data breaches	Companies are obliged to inform the authorities and possi-bly the people concerned in the event of a security breach resulting in access to, disclosure or loss of personal data.
Privacy by design/by default	Companies must integrate data protection into the design of a product or service (privacy by design). In addition, the default settings of the services or software must guarantee the highest level of confidentiality and security without user intervention (privacy by default).
Presence of a data protection officer	Companies are required to appoint someone who is responsible for the protection of personal data (data protection officer) to ensure compliance with current regulations.
Sanctions	Companies are subject to sanctions for violating data pro-tection laws.
Right to transparency for individuals	Companies must inform individuals about how their personal data is being collected, used and shared.
Right to access	Upon request, companies are obliged to provide people with a copy of the personal data being held on them.
Right to rectification	Upon request, businesses are required to correct or update inaccurate or incomplete personal information held on an individual.
Right to erasure	Upon request, companies have an obligation to delete individuals' personal data.
Right to restrict processing	In certain specific circumstances, companies must temporarily restrict the processing of an individual's data if requested to do so.
Right to portability	Upon request, companies have an obligation to provide individ-uals with their personal data in a commonly used format and transfer it to another company.
Right to object	Companies must allow individuals to object to the processing of their personal data for legitimate reasons.
Right not to be subject to a decision based solely on automated processing	Individuals can demand that the automated processing of their data leading to a decision by companies be reviewed by an individual.

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

Comparative table

	Switzerland	European Union	United Kingdom	Norway	Iceland	Türkiye	United States	Canada	Brazil	Tunisia	Morocco	South Africa	United Arab	Russia	India	China	Hong Kong	Japon	South Korea	Taiwan	Singapore	Thailand	Vietnam	Australia
State where an adequate level of data protection is guaranteed **(Link)**	●	●	●	●	●			●																
Information obligation	●	●	●	●	●	●	●	●	●	●	●	●	●	●	○	●	●	●	●	●	●	●	●	●
Activity log	●	●	●	●	●	●	○	●	●	●	●	●							○			○	●	
Impact analysis	●	●	●	●	●	○	○	●	●			●	○	○	○	●							●	
Consent for processing sensitive data	●	●	●	●	●	●	○	●	●	●	●	●	●	●		●	○	●	●	●	●	●	●	●
Notification of data breaches	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●			●	●	●	●	●	●
Privacy by design/ by default	●	●	●	●	●	○	○	●	○														●	
Presence of a data protection officer	○	●	●	●	●	○	○	●	●	○	○	●	○	○	○	●			●		●	○	○	
Sanctions	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Right to transparency for individuals	●	●	●	●	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●	●	●	●	●
Right to access	●	●	●	●	●	●	○	●	●	●	●	●	●	●	●	●	●		●	●	●	●	●	●
Right to rectification	●	●	●	●	●	●	○	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Right to erasure	●	●	●	●	●	●	○	●	●	●	○	●	●	●	○	○	○	●	●	○	○	●	●	○
Right to restrict processing	●	●	●	●	●	●	○	●	●	●		●	●			●		○	●			●	●	
Right to portability	●	●	●	●	●		○		●	●			●			●			●			●	●	
Right to object	●	●	●	●	●	●	○	●	●	●	●	●	●		●	●	○	○	●		●	●	●	
Right not to be subject to a decision based solely on automated processing	●	●	●	●	●	○	○	●	●	●		○	●	○		○			●					

● = *Yes*
○ = *Yes in certain cases, states or provinces.*

Always refer to the regulations in effect. The information here is given for information purposes only.
More information should always be obtained by reading the regulations in effect for the country concerned.

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0

Steps for optimal data management and regulatory compliance

Identify the markets in which the company is active. First of all, a list should be compiled of the countries, regions or states in which the company is active. Next, it is necessary to identify the types of commercial or management activities conducted by the company in these regions and see if they are subject to the regulations in effect.

Read and understand the regulations in effect in countries where the company is active. Regulatory frameworks vary by region and type of business activities. It is essential to find out about the regulations in effect in the countries where the company is active to ensure compliance with the applicable laws.

Only collect necessary data. It is necessary to ensure that any data is processed lawfully, and minimise data collection to that which is strictly necessary, limiting it to the purpose of processing agreed by the company and stated upon its collection. It is also necessary to specify how long this information will be kept.

Inventory and map data held by the company. An inventory makes it possible to identify any information the company should not have in order to be compliant and apply the data processing that is required.

Manage the data lifecycle. It is important to determine how long the data collected or produced will be needed and agree on a data deletion date. When the data is no longer needed for processing purposes, it must be destroyed or anonymised.

Develop and apply a transparency policy for data processing. Just as when data is collected, it is essential to be transparent about the data being held, the purpose of its processing, and its intended use by the company or partners.

Protect data which is collected. It is important to put in place all necessary measures to protect the data being held and managed by the company. This especially concerns technical measures and the training of any person with access to the data

For more information, refer to the cyber risk guide.

Geneva, a pioneering canton in the right to digital integrity
On 18 June 2023, 94.21% of people from Geneva accepted a modification to the constitution of the Republic and canton of Geneva, in which a fundamental right was introduced aimed at protecting citizens' digital integrity, mainly within the framework of relationships with public administrations.

This document © 2024 by the State of Geneva is licensed under CC BY-SA 4.0