

All countries

Other considerations

Asia

China

Other considerations With China's fast development in the cyber security and data protection regime, privacy topics are gaining more importance. Offline and online content censorship adds further complexities. Compliance efforts are strongly recommended which may include e.g. good data governance including data inventory and classification system, organisational set up (like a CISO and DPO) with clear functional guidance, internal procedures and protocols (like privacy policies, data classification, IT guidance and use of company VPN), and legal tools to manage data export topic (which is of particular sensitivity for international companies). In this context, think carefully about your IT deployment strategy for China is critical so as to streamline future compliance investment.

Hong Kong

Collection of personal data for direct marketing:

- There are requirements of notification and consent from data subjects to enhance protection of consumers data privacy rights against unwanted direct marketing activities, eg data subject is entitled to exercise his/her opt-out right and data users must comply with the request.

Data export restriction (not yet in force):

- Export of personal data outside of the jurisdiction will be subject to conditions, eg data subjects written consent or whether the data user or the Commissioner has reasonable grounds to believe that the personal data will be transferred to a jurisdiction that provides a similar degree of protection as Hong Kong.

Singapore

Organisations will need to determine the most appropriate form of notification to meet their business needs.

United Arab Emirates

Apart from a situation where there is a legal requirement to do so, the unauthorised use of personal data may qualify as a criminal offence under the UAE Penal Code and/or Federal Decree Law No. 34 of 2021 on Combatting Rumors and Cybercrimes .

Therefore, matters including but not limited to the processing of employee's information, recording of any conversations, using video surveillance equipment and recordings created, or even taking pictures during events and the use of the same for any purposes should be handled carefully. Ideally and, where possible, consent of the concerned person should be obtained prior to any form of processing of personal data. It is noteworthy that the DP Law, contrary to the GDPR, does not include a 'legitimate interest' of the data controller as a potential reason for permitted processing of personal data.

Europe

Austria

Data controllers must ensure full compliance with GDPR requirements. This includes having all the required documentation in place at the disposal of the DPA in case of control, to demonstrate compliance (record of processing activities, privacy policies, data processing agreements, consent forms, data transfer agreements, data retention policy...) and procedures (PIAs, privacy by design and by default, data subjects' rights, IT security...).

It must also be noted that the DPA generally follows the recommendations of the former Working Party 29 (now the European Data Protection Board), which takes a strict approach on the interpretation of GDPR requirements.

Since July 10, 2023, the "Adequacy decision for the EU-US Data Privacy Framework" has given another option for the transfer of personal data to the USA. Adequacy decisions and standard data protection clauses are two of the options for lawful international data transfers, alongside the EU-US Data Privacy Framework. There are also others, such as the explicit consent of the data subject in individual cases or the necessity for the performance of a contract with the data subject.

Finally, there remain areas where Austrian law has specific requirements or diverging regulations, in addition to GDPR requirements. This is notably the case with the principle of warning instead of punishment, in the event of first-time and usually less serious data protection breaches or violations.

Czech Republic

Moreover, there are specific provisions regarding the monitoring of employees set out in the Czech Labour Code. Open or concealed surveillance (monitoring) of employees, interception (including recording) of their telephone calls, checking their electronic mail or postal consignments addressed to a certain employee, may be performed only if there is a serious cause consisting in the employer's nature of activity. The employer shall directly inform the employees of the scope and methods of such monitoring.

Personal data can only be transferred outside of the EEA where certain safeguards are in place or if the country to which the data is being transferred is deemed by the European Commission to give adequate protection to personal data. Personal data may also be exported from the EU (not the EEA) to the US where the importer has certified under the EU-US Privacy Shield.

As regards privacy in the electronic communications sector, due to a specific implementation of Directive 2002/58/EC of the European Parliament and of the Council, when a website controller wishes to use cookies it can do so based on opt-out principle rather than opt-in prescribed by the Directive.

England & Wales

Personal data can only be transferred outside the EEA where certain safeguards are in place or if the country to which the data is being transferred is deemed by the European Commission to give adequate protection to personal data. While consent may be used to legitimise the export of personal data to third countries in limited circumstances, in most cases, contracts will be required. These may be in the form of EC Model Clauses or Binding Corporate Rules. Personal data may also be exported from the EEA to the USA where the importer has certified under the EU-US Privacy Shield.

The UK's data protection law stems from the EU's General Data Protection Regulation, and its own Data Protection Act 2018. The UK has made provision for a new UK GDPR to be created at the end of the transition period following the UK's exit from the EU. This mirrors the GDPR but removes EU-specific references including to regulator cooperation and the European Data Protection Board. The UK has also made transitional provision for data flows to continue uninterrupted to the EEA, countries currently benefitting from an EU Adequacy Decision, Gibraltar and to the US under the Privacy Shield. Data flows to the UK from the EEA may be disrupted on exit unless a suitable GDPR data transfer mechanism applies, or a separate agreement is reached on the question of data transfers between the EU and the UK. Cross-border businesses may also need to consider the location of their Lead Supervisory Authority and Data Protection Officer (if they have one), as well as whether or not they need to appoint a representative in the UK and/or the EU.

France

Data controllers must ensure full compliance with GDPR requirements and other applicable privacy regulations (notably e-privacy Directive). This includes having all the required documentation in place at the disposal of the CNIL in case of control, to demonstrate compliance (record of processing activities, privacy policies, data processing agreements, consent forms, data transfer agreements etc) and internal procedures (PIAs, data retention policy, privacy by design and by default, data subjects' rights, data breaches, etc).

It must also be noted that the CNIL generally follows the recommendations of the European Data Protection Board (EDPB), which takes a strict approach on the interpretation of GDPR requirements.

In addition, specific requirements resulting from the French Data Protection Act (Loi Informatique et Libertés) have been implemented. This is notably the case for the processing of employee data, sensitive data (including health data), as well as data relating to criminal offences and convictions. French law also has a specific regime applicable to the hosting of health data collected in the course of prevention, diagnosis or care activities which is subject to a prior mandatory certification process.

The CNIL also issues guidelines on specific data protection related topics. In this respect, in 2023, draft guidelines relating to (i) the development of mobile applications and (ii) the creation of datasets involving personal data used to train AI systems have notably been published, pending a final version in 2024.

Germany

In general, all data controllers must ensure full compliance with GDPR requirements. This includes among others having all the required documentation in place at the disposal of the respective competent regulator in case of an inspection, to demonstrate compliance (eg record of processing activities, privacy policies, data processing agreements, consent forms, data transfer agreements, etc) and procedures (PIAs, privacy by design and by default, data subjects' rights, data breaches, etc.). If data controllers do not comply with this, they may be subject to fines in individual cases.

Personal data can only be transferred outside the EEA where certain safeguards are in place or if the country to which the data is being transferred is deemed by the European Commission to give adequate protection to personal data. While consent may be used to legitimise the export of personal data to third countries in limited circumstances, in most cases, contracts will be required. These may be in the form of Standard Contractual Clauses (SCCs) or Binding Corporate Rules.

With regard to data transfers to the U.S., on 10 July 2023 the European Commission adopted an adequacy decision for data transfers to data importers in the U.S. participating in the "EU-US Data Privacy Framework" ("DPF"). The adequacy decision, which has been effective immediately, concludes that the U.S. provides an adequate level of protection compared to the EU. The adequacy decision follows the signing of U.S. Executive Order (E.O.) 14086 of 7 October 2022, on Enhancing Safeguards for United States Signals Intelligence Activities, which introduced new mandatory safeguards to address the issues raised by the CJEU in its Schrems II decision invalidating the EU-US Privacy Shield (predecessor to the DFP).

For U.S. companies with active Privacy Shield certification, the requirement for initial self-certification under the DPF is eliminated. From now on, they must comply with the principles of the DPF, update its privacy policies and recertify within the usual due date.

Data transfers to the U.S. are now subject to less risk.

- Data transfers to U.S. companies are currently permitted under the DPF. Special precautions for data transfers are therefore currently no longer mandatory.
- In addition to the DPF, however, an agreement on commissioned data processing is still required for a data processor. Here, the SCCs could be used, which fulfill the requirements of Art. 28 GDPR.

It remains to be seen whether the DPF will be upheld or whether the ECJ may declare it as invalid in the future.

Finally, there remain areas where German law will have specific requirements, in addition to GDPR requirements. This is notably the case eg for the processing of employee data and sensitive data (including health data).

Hungary

For data transfers within the EU, no additional measures would be required regarding the direct applicability of the GDPR in every EU member state. However, where a data controller occupies a service provider acting as data processor, their relationship shall be governed by an agreement. This agreement or contract is subject to the minimum criteria laid down under the GDPR.

In the case of non-EU data transfers, those specific situations are defined when such transfers may be carried out. It shall be considered whether there is an adequacy decision of the EU and if there is no such decision, additional guarantees by means of contractual agreements will have to be provided.

In order to prevent the unlawful processing of personal data, the Authority may order - in the form of a provisional measure - the rendering of electronic data inaccessible temporarily, the publication of which prompted the Authority to open administrative proceedings for data protection or regulatory inspection.

Ireland

Personal data can only be transferred outside the EEA where certain safeguards are in place or if the country to which the data is being transferred is deemed by the European Commission to give adequate protection to personal data. While consent may be used to legitimise the export of personal data to third countries in limited circumstances, in most commercial situations it will not be a practical basis for transfer. In June 2021, the Commission published its decision on the new standard contractual clauses (SCCs) for the transfer of personal data from the European Union to third countries, and the template SCCs themselves. The new SCCs addressed the CJEU's decision in Schrems II by incorporating a number of terms designed to ensure an appropriate level of protection for personal data transferred to third countries from the EEA. The Commission confirmed that there would be an 18 month transition period, during which time companies can continue to transfer personal data to third countries using the existing SCCs. As of 27 September 2021, the previous SCCs can no longer be used for new contracts or new processing activities.

Cross-border businesses may also need to consider the location of their Lead Supervisory Authority and Data Protection Officer (if they have one), as well as whether or not they need to appoint a representative in Ireland and/or the EU.

The DPC actively enforces the rules around direct marketing and frequently prosecutes breaches.

Italy	<p>The main areas where the Italian Data Protection Code provides for specific requirements are the following: processing of employees' personal data, processing of genetic data, biometric data or data concerning health, the legal basis applicable to processing of personal data (including health and genetic data) for the purposes of scientific research in the medical, biomedical or epidemiological field; processing of personal data relating to criminal convictions and offences (for which a Decree of the Ministry of Justice is expected to be issued soon); rights concerning deceased people; cases where data controllers may refuse to comply with a request of exercise of rights from the data subject. Additionally, in 2021 the Italian Data Protection Code was amended to include a high-speed reporting system for revenge porn victims.</p> <p>The Italian Data Protection Code contains also the provisions implementing the ePrivacy Directive (Directive 2002/58/EC), including the rules governing placement of cookies, processing of traffic and geolocation data.</p> <p>Finally, in 2023 Legislative Decree No. 24/2023 implementing the Directive (EU) No.1937/2019 on whistleblowing was adopted, including also rules concerning data protection.</p>
Netherlands	<p>Personal data can only be transferred outside the EEA where certain safeguards are in place or if the country to which the personal data is being transferred is deemed by the European Commission to ensure an adequate level of protection for personal data. Under the GDPR, accessing personal data from outside the EEA is considered a data transfer as well.</p> <p>Following the outcome of the Schrems II-case (i.e. the invalidation of the adequacy decision regarding Privacy Shield) by the European Court of Justice, the Dutch DPA has been reluctant to indicate if and how it will investigate and enforce non-compliant data transfers to the US pending further guidance from the European Data Protection Board and/or new legislation. Pursuant to the guidelines from the European Data Protection Board, Dutch companies transferring personal data to the US are advised to perform risk-assessments per data transfer and ensure that appropriate safeguards (e.g. the use of standard contractual clauses) are present. As of September 2021, parties need to apply the new EU model clauses (SCCs) when transferring personal data to a country without an adequate level of protection. These new SCCs offer more options and better protection for the data transfer.</p> <p>Although the foregoing still applies at the moment, note that the European Commission has adopted a new adequacy decision for EU-US data flow. Based on the recently adopted adequacy decision, personal data can be transmitted securely from the EU to US companies that participate in the Framework, eliminating the need for implementing extra data protection measures. For companies that do not participate in the Framework, SCCs will reportedly still be required for transfers of personal data to the United States. This does also apply to other countries that do not have an adequacy decision or other mechanisms in place. Transfers of personal data to such countries will then still require the use of SCCs.</p> <p>Specific data protection and privacy legislation (e.g. further notification requirements and industry-specific enforcement guidance) may apply to companies in specialized markets, such as healthcare, energy, fuel, water supply and internet access providers. Companies with user data that may be valuable to public authorities (e.g. for a criminal investigation), such as police and public prosecutors, should also ensure that they have appropriate policies ready to deal with such data requests.</p>

Poland

Personal data can only be transferred outside the EEA where certain safeguards are in place or if the country to which the data is being transferred is deemed by the European Commission to give adequate protection to personal data. While consent may be used to legitimise the export of personal data to third countries in limited circumstances, in most cases, contracts will be required.

These may be in the form of EC Model Clauses or Binding Corporate Rules.

As regards the data exports to the USA given the CJEU judgment in the Schrems II case certification of the data importer under the EU-US Privacy Shield is not sufficient any more.

Portugal

Personal data can only be transferred outside the EEA where certain safeguards are in place or if the country to which the data is being transferred is deemed by the European Commission to give adequate protection to personal data.

While consent may be used to legitimise the export of personal data to third countries in limited circumstances, in most cases, contracts will be required. These may be in the form of EC Model Clauses or Binding Corporate Rules.

The national law specifies rules about labor and employment data processing activities, video surveillance, obligation of DPO for public and private entities, among others. The national law also establishes specific types of crimes and correspondent sanctions.

The CNPD has publish the Regulation for Data Protection Impact Assessment and its additional criteria.

The Portuguese's data protection law stems from the EU's General Data Protection Regulation, and its own Data Protection Law.

Also, in Portugal is applicable the Law 41/2004, of 18 August, Protection of Personal Data and Privacy in Telecommunications, which transposes into national law Directive 2002/58/EC of the European Parliament and of the Council of 12 July on the processing of personal data and the protection of privacy in the electronic communications sector.

Additionally, on cybersecurity legal requirements, Portugal has the Law no. 46/2018 of 13 August establishing the Legal Framework for Cyberspace Security, transposing Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. And the Decree-Law no. 65/2021, of 30 July, which regulates the Legal Framework for Cyberspace Security and defines the obligations in terms of cybersecurity certification in implementation of Regulation (EU) 2019/881 of the European Parliament, of 17 April 2019.

Slovakia

Along with GDPR, Act no. 18/2018 Coll. on Personal Data Protection regulates the data protection. The Act follows GDPR and applies analogical rules also in situations falling outside the scope of GDPR.

Moreover, there are specific provisions regarding monitoring of employees set out in the Slovakian Labour Code. Open or concealed surveillance (monitoring) of employees, interception (including recording) of their telephone calls, checking their electronic mail or postal consignments addressed to a certain employee, may be performed only if there is a serious cause consisting in the employer's nature of activity. The employer shall directly inform the employees of the scope and methods of such monitoring.

Personal data can only be transferred outside of the EEA where certain safeguards are in place or if the country to which the data is being transferred is deemed by the European Commission to give adequate protection to personal data.

Spain

Personal data may be transferred outside the EU when the importing state has an adequate level of protection recognized by the European Commission or when adequate safeguards are provided, such as binding corporate rules or, more commonly, standard contractual clauses (approved by the European Commission in 2021).

It will also be necessary to carry out a transfer impact assessment to determine the risks involved, which, if considered high, will require additional safeguards, as was the case, for example, when transferring data to the United States, as established by the CJEU in its July 2020 ruling in case C-311/18 (better known as Schrems II).

South America

Brazil

Brazil has a strong Data Privacy regulation, the LGPD (Law 13.709/2018), which is very similar to the GDPR. Nonetheless, it is imperative a Data Privacy Compliance program in Brazil, adequate to the LGPD requirements. In addition, a foreign company must have an appointed DPO. The DPO can be an employee with substantial knowledge, an external (natural or legal) person, or an external law firm. Privacy regulations are on the spotlight over the last months, as administrative sanctions are about to be applied. There is also the possibility for Procon, Ministério Público and Judiciary to apply additional sanctions. Sanctions can be a warning, indicating the deadline for the adoption of corrective measures; a fine up to 2% (two percent) of the revenues of the legal entity group or conglomerate in Brazil, limited to R \$ 50,000,000.00 (fifty million reais) for infringement; a daily fine; publicization of the infraction; a range of prohibitions to use the internal data base until regularization or up to 1 (one) year.

Data Subjects must also be indemnified over breaches involving their own data.