TaylorWessing

All countries

Notification requirements

Asia

China	Yes. A company shall, when collecting personal information, present its privacy policy disclosing the purpose, means and scope of collection and use of personal information, and it shall secure prior consent from the data subject. In case of a data breach, a company is subject to a general obligation to notify the data subject and competent regulators.
Hong Kong	No requirement to register with or notify any authorities of data processing.
Singapore	An organisation must inform individuals of the purposes for the collection, use or disclosure of the personal data on or before collecting the personal data, and on request by the individual, the business contact information of a person who is able to answer on behalf of the organisation the individual's questions about the collection, use or disclosure of the personal data. If there is a data breach incident that is likely to cause significant harm to the affected individuals, or affects a significant scale of individuals, the relevant organization is legally required to notify the Personal Data Protection Commission and any affected persons as soon as it is practicably able to.
United Arab Emirates	Generally speaking this is not applicable in the UAE. But there are a few exceptions.

Europe

Austria	Following applicability of GDPR, there is no general requirement to notify planned or ongoing data processing involving personal data to the DPA. Rhe Austrian Data Protection Act (Datenschutzgesetz) also supplements the GDPR in Austria. The controller, however, must notify (inform) the processing to the data subjects. Nevertheless, specific situations can occur where notification to, consultation with, or authorization from the DPA is required. For instance, GDPR has introduced a notification requirement in case of a personal data breach. Such breaches must be notified to the DPA within 72 hours (in case this timeframe is not met, such delay must be documented and justified), and, depending on the severity of the breach, also notified to the data subjects whose data have been affected by the breach.

Czech Republic	In the Czech Republic, this area is governed by GDPR. Moreover, the Czech Adaptation Law is effective since April 2019 that specifies certain general rules in more detail and lays down several differences from the general regime under GDPR. For example, controllers are relieved from certain obligations (including informing the data subjects) in case of data processing for purposes of journalism, and age limit relating to conditions applicable to child's consent in relation to information society services has been set to 15 years. Further, this adaptation legislation limits/precludes fines against public institutions. There is no general requirement to notify planned or ongoing data processing to the Office for Personal Data Protection. The controller, however, must notify (inform) the processing to the data subjects. Nevertheless, specific situations can occur where notification to, consultation with, or authorisation from the Office is required. On the other hand, GDPR has introduced a notification requirement in case of a personal data breach (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons). Such breaches must be notified to the Office for Personal Data Protection within 72 hours (in case this timeframe is not met, such delay has to be justified), and, depending on the severity of the breach, to the data subjects whose data have been affected by the breach.
England & Wales	The GDPR did away with an annual notification requirement, however, the UK government introduced a new annual data protection fee which ranges from £40-£2,900 depending on the size of the organisation in question. The ICO has set up a self-assessment tool to help organisations work out whether and what they need to pay. The ICO is actively enforcing for non-payment which can lead to fines. There are additional notification requirements in relation to data breaches under the GDPR and the NIS Regulations.
France	With the entry into force of the GDPR, notification of processing activities to the CNIL is no longer required: notification formalities have been replaced by an "accountability" principle. In some specific cases however (e.g., for some processing activities in the health sector), it is still necessary to obtain a prior authorisation from the CNIL. On the other hand, GDPR has introduced a notification requirement in case of breach of personal data. Depending on the severity of the breach, such breach must may need be notified to the CNIL within 72 hours to the data subjects whose personal data have been affected.

Germany	With the entry into force of the EU GDPR, notification of processing activities to the respective competent regulator is no longer required; notification formalities have been replaced by an accountability principle. On the other hand, GDPR has introduced a notification requirement in case of breach of personal data. Such breaches must be notified to the respective competent regulator without undue delay and, where feasible, not later than 72 hours since the breach occurred and, depending on the severity of the breach, to the data subjects whose data have been affected by the breach without undue delay. In addition, the controller shall consult the competent regulator prior to processing where a data protection impact assessment under Art. 35 GDPR indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. In specific situations, there is an obligation to appoint a Data Protection Officer and to notify the respective competent regulator thereof.
Hungary	With the entry into force of the GDPR regulation the Data Protection Directive 95/46/EC has been replaced. Under the new regulation the notification of processing activities to the data protection authority is no longer an obligation. However the GDPR regulation has introduced a notification requirement as a replacement, in case of breach of personal data. In case of breaches the authority must be notified within 72 hours. Depending on the severity of the breach, those data subjects (natural persons) whose data have been affected by the breach, shall be notified as well (eg in case of bank account numbers or passwords have been made public). Incidents can currently be reported either through the incident reporting interface available in Hungarian on the authority's website, or by completing the authority's Hungarian-language form. This form can be submitted via the 'Client Gate' ('Ügyfélkapu'), the Hungarian Government’s electronic platform for communication with local authorities. Utilizing the Client Gate requires preliminary registration and personal identification at a local government service office ('Kormányablak'). Given the strict 72-hour deadline for reporting, in cases where the reporter is not proficient in Hungarian (and there is no time for translation) and/or does not have access to the official client portal, our office's services are recommended. We are legally authorized to act on behalf of clients in the reporting process, based on a power of attorney provided by the client.
Ireland	The EU General Data Protection Regulation 2016/ 679 (GDPR) together with the Data Protection Acts 1988 – 2018 comprise the legal framework governing data protection and privacy. These measures require personal data breaches to be notified to the DPC. Where an organisation has appointed a Data Protection Officer under the GDPR, this appointment should also be notified to the DPC. The European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 introduced notification requirements to the National Cyber Security Centre, which relate to operators of essential services and digital service providers, which can also apply to data breaches.

Italy	Following the entry into force of the GDPR, the Italian Data Protection Code (Legislative Decree No. 196/2003) does not provide for notification formalities applicable to certain processing activities. Indeed, notification formalities were provided under the former legislation, but were repealed by Legislative Decree No. 101/2018, which adapted the Italian Data Protection Code to the GDPR. The GDPR however introduced the obligation to notify data breaches to the competent supervisory authority within 72 hours from the discovery of the personal data breach, unless it is unlikely that the data breach will result in a risk to the rights and freedom of the data subjects. The notification to the Garante must be made by means of the online service available on the Garante's website, which also provides several tools to support data controllers in their obligations in the event of a data breach (e. g. a self-assessment procedure to identify the actions to be taken). Additionally, the Italian Data Protection Code provides that the authorization of the Garante must be obtained in some specific cases (such as, secondary processing of particular categories of personal data for purposes of scientific research or statistic purposes).
Netherlands	No general notification requirements for data processing activities. However, each controller must maintain a record of processing activities, which needs to be provided to the data protection authority on request). Notification requirements are in place for data breaches and for the appointment of a Data Protection Officer. Notifications can be made electronically via forms made available by the Dutch Data Protection Authority on its website and are free of charge.
Poland	In principal all limited liability companies, simple joint stock companies and joint stock companies are data controllers. 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 Personal Data Protection Office 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. In specific situations, there is an obligation to appoint a Data Protection Officer. There are no notification requirements for data processing activities. Notification requirements are in place for data breaches and for the appointment of a Data Protection Officer. In case of a breach of duties relating to personal data protection, the personal data administrators should notify the President of the Personal Data Protection Office of such breach – the relevant notification may be made via internet platform using the provided electronic notification form. The notification should follow within 72 hours since the breach occurred.

Portugal	In Portugal, the national legislation is Law 58/2019, 8 August, which ensures the implementation of the GDPR in the Portuguese legal system. The GDPR establishes that fines may be imposed of up to € 10,000,000.00 or up to € 20,000,000.00 (depending on the subject matter of the administrative infraction) or up to 2% or 4% of its annual worldwide turnover corresponding to the previous financial year, whichever is higher. The Portuguese regulator, through Law nº. 58/2019 of 8 August, which ensures the implementation of the GDPR in the Portuguese legal system, establishes a graduation of administrative offences and, consequently, of fines. Thus, there are very serious administrative offences, which may lead to the application of fines amounting to: • Large companies: from € 5,000.00 to € 20,000,000.00 or 4% of the annual worldwide turnover, whichever is higher; • SMEs: from € 2,000.00 to €2,000,000.00 or 4% of the annual worldwide turnover, whichever is higher; and • Natural persons: from € 1,000.00 to € 500,000.00. In the case of serious administrative offences, they may lead to the application of fines amounting to: • Large companies: from € 2,500.00 to € 10,000,000.00 or 2% of the annual worldwide turnover, whichever is higher; • SMEs: from €1,000.00 a € 1,000,000.00 or 2% of the annual worldwide turnover, whichever is higher; e, • Natural persons: from € 500.00 to € 250,000.00.
Slovakia	Following the adoption and effectiveness of GDPR, there is no general requirement to notify planned or ongoing data processing to the Office for Personal Data Protection. The controller, however, must inform the data subjects about processing. Still, there may arise situations where notification to, consultation with, or authorisation from the Office is required. On the other hand, GDPR has introduced a notification requirement in case of a personal data breach. Such breaches must be notified to the Office for Personal Data Protection within 72 hours (in case this timeframe is not met, such delay has to be justified), and, depending on the severity of the breach, to the data subjects whose data have been affected by the breach.
Spain	Since GDPR it is not necessary to notify the files to the AEPD. However, it is necessary to notify security breaches affecting personal data as soon as possible and, in any case, within 72 hours of knowledge. Likewise, it would be necessary to notify any variation in the binding corporate rules previously approved by the AEPD, if applicable.

South America

Brazil	The LGPD distresses the need of an open channel for the Data Subject and any requests shall be replied within 15 (fifteen) days. In addition, in case of Data Incident or any substantial breach, the LGPD establishes that a communication must be made within a reasonable period, as defined by the ANPD. Currently, the ANPD recommends a period of 2 (two) business days for the communication, but this deadline might be modified.