MLS / Company Secretary

GDPR: THE RULE, YOUR OBLIGATIONS AND OUR COMMITMENT TO HELP YOU

1 OUTLINE

The EU General Data Protection Regulation (GDPR) came into force in Europe on 25 May 2018 and it brought considerable changes to data protection law in Europe and across the European Economic Area (EEA) more widely. It includes significantly greater fines for breaches of up to €20 million or 4% of the total worldwide annual group turnover. Failure to comply with the GDPR also carries risk in the context of adverse publicity as it can lead to reputational damage and lost customer trust, civil liability or punitive damages for employment related breaches and business continuity issues. In addition, directors and senior managers can face criminal charges resulting in imprisonment and substantial penalties if found guilty of breaching the GDPR.

Your company should actively prepare for these requirements to ensure that you are compliant. This involves teaching/training staff on new obligations, reviewing policies and contracts as well as ensuring awareness of the transparency requirements. The GDPR is applicable if data processing takes place. This includes processing of employee personal data as well as personal data relating to all other living individuals.

We have identified some of the biggest changes to the current law. We have kept these brief but there are many more you will need to familiarise yourself with.

2 WHAT TO DO FROM NOW

2.1 Check if your company is caught by the GDPR

The GDPR applies to your company if:

- You have a physical presence in the EU; or
- You are not EU based but you process data that relates to individuals in the EU in the context of offering goods or services or by monitoring behaviour.

Check if your responsibilities have changed under the GDPR:

- If you are a data controller, you decide the manner and reason for processing personal data. Under the GDPR you are required to ensure that contracts with your data processor are GDPR compliant;
- If you are a data processor, you will act on behalf of the data controller. Under the GDPR you must now document your activities of processing personal data.

2.2 Understand the changes introduced by the GDPR

a) Lawful processing and consent

- It is necessary to identify and record the lawful basis for processing. If processing is carried out with consent from the individual, the consent must have been given clearly, unambiguously and with an action to opt-in.
- Document all consents.
- It is difficult for consent to be freely given by an employee because of the imbalance of power between employer and employee. This means that consent alone is unlikely to be a valid basis for processing HR data, so employers should consider other grounds for lawful processing, such as being in the legitimate interests of the business.
- For employers, transparency in processing data is achieved by keeping the employee or prospective employee informed before data is collected and where any subsequent changes are made. **b) Accountability and demonstration**

- A key change relates to the obligation to demonstrate compliance with GDPR. The requirement to register with the Information Commissioner's Office has been discarded. Instead you have to keep full records of any data processed, including the type of data and the purpose it is used for.
- Data controllers must only process personal data which is necessary for each specific purpose. For employers, this means collecting enough data to achieve their purpose but not more than needed.
- You also need to give much more detailed notices to people you collect information from.
- Internal compliance programs, further data protection policies and staff training are all steps to take. Carrying out regular tests on the implementation and retaining the results can be used as evidence of continuous compliance.

c) Obligation to inform data subjects of the data you have collected

The previous data protection regime required organisations to inform individuals when personal data had been collected. The GDPR imposes requirements to supply further details to individuals. Policies on this should therefore be reviewed and updated.

d) Access to information

The GDPR removes the right to charge an amount for accessing personal data and companies are now required to supply the data within one month of receiving a request.

If appropriate, it is recommended that self-service access systems are put in place.

➢ **Next step: Are you comfortable dealing with subject access requests? Do you know what you have to disclose and what you can withhold?**

e) Inaccurate data and erasure

Individuals can under GDPR require companies to correct inaccurate information. This includes a requirement on the company to communicate the rectification to third parties who have received the inaccurate data.

Subject to limited situations, GDPR provides a right to have personal data erased and removes the previous requirement of distress and damage as a result of the processing.

e) Portability

Data portability enables data subjects to transfer their personal data in a commonly-used electronic format from one data controller to another, enabling people to switch between service providers more easily.

A request must be responded to within one month and information must be provided free of charge.

➢ **Next step: Do you have a system in place to deal with such request?** **f)**

Notifying breaches

GDPR imposes an obligation to notify a data breach to the authority if the breach is capable of affecting the rights and freedoms of the individual. Each breach should be assessed to ascertain if a notification is appropriate. The individual should also be notified if the breach is of a high-risk nature.

➢ **Next step: You should ensure you have the right procedures in place to detect, report and investigate a personal data breach. You should also check that agreements with your suppliers require them to tell you immediately if there has been a breach.**

g) Data Protection Officers

Public companies and companies carrying out extensive data processing must appoint a Data Protection Officer who will supervise and monitor compliance. He/she will also be the main point of contact for the authority and individuals.
Other companies may appoint a Data Protection Officer and should in any event be satisfied that they have resources to comply with GDPR obligations.

You should consider whether you need to appoint a DPO.

h) Data Processing Agreements (DPA) -

What is a DPA :

A DPA is a contract between data controllers and data processors or data processors and subprocessors. Under the GDPR a data controller is essentially the owner of the personal data in question. The data controller likely collected the data and determined how and why it will be processed. Data controllers often use data processors to assist them with a variety of tasks.

These agreements are intended to ensure that each entity in the partnership is operating in compliance with the GDPR or other applicable privacy laws in order to protect the interests of both parties.

For example, if you collect personal data from the users on your website, then use a third-party processor to handle some aspect of your business strategy, you should want to know that data processor is operating within GDPR compliance and doing what they should be doing with the important data of your users.

- What must be included in a DPA ?

- What information is being processed.
- How long that information will be processed
- Why this information is being processed
- The rights and responsibilities of the data controller
- That the data processor should only act according to written instructions from the data controller
- That data processing is done confidentially
- That proper security measures are in place during every step of data handling
- Subprocessors only be used with the data controller's knowledge and consent
- Data controllers and processors should work together to resolve subject access requests
- Data controllers and processors should work together to protect the rights and privacy of data subjects
- Data processors must inform data controllers of data breaches
- Data processors should assist data controllers in data protection impact assessments where applicable
- Data processors should erase or return the personal information from the data controller after the contract is complete
- Both data controllers and processors should be prepared for audits or inspections and assist one another as needed to demonstrate compliance
- Data processors and controllers should be on the lookout for any practices that break GDPR compliance and notify the other so that corrections can be made
- The data processor shall have a Data Protection Officer appointed as required by the GDPR The data processor shall keep records of processing activity

3 IMPLEMENT GDPR

- Consider the geographical location/s of your business
- Know and understand the data held within your business (specifically where it came from and who it is shared with)

- Carry out an audit of data protection policies and practices, including existing employment contracts, staff handbooks and employee policies, and update where necessary
- Make sure there is transparency over the nature of HR data processing relating to the data used, the purposes for which it is used and where it is processed.
- Where you have relied on consent to justify processing of HR data, consider an alternative and ensure this is recorded.
- Review privacy procedures and ensure that all rights granted to individuals under GDPR are accounted for
- Ensure consents from individuals are recorded/documented and that they have been given in a compliant manner
- Incorporate policies for privacy policies for children and consents by parents/guardians
- Implement appropriate privacy notices
- Review procedure for accessing information
- Review agreements with suppliers
- Establish a data breach policy and create a breach reporting mechanism
- Train staff on obligations
- Possibly appoint a Data Protection Officer.
- Review or make a Data processing Agreement

Businesses should actively take steps to ensure that they are compliant. This involves training staff on new responsibilities, reviewing policies, systems and contracts as well as ensuring awareness of the transparency requirements.

4 HOW WE CAN HELP?

The Consultant Team of MLS Company Secretary can help you with:

- Reviewing policies and procedures.
- Drafting your Data Processing Agreement
- Reviewing existing contracts Staff training.
- Identify operation *vs* legal questions and gather competitive fees estimates for legal advice if necessary.

Please contact: Hélène Canard-Duchêne (Singapore)
hcd@mlscompanysecretary.com
+65 9396 9193

Maëva Slotine (Hong Kong)
ms@mlscompanysecretary.com
+852 26393680