25 March 2020
Global Tax Alert

Luxembourg: Data protection and impact of COVID-19

EY Tax News Update: Global Edition

EY's Tax News Update: Global Edition is a free, personalized email subscription service that allows you to receive EY Global Tax Alerts, newsletters, events, and thought leadership published across all areas of tax. Access more information about the tool and registration here.

Also available is our EY Global Tax Alert Library on ey.com.

The impact of the COVID-19 pandemic on the everyday life of Luxembourg companies is dramatic. Protecting employees, customers and business partners from infection is a new, urgent challenge for many companies.

With the further progression of the dissemination, the question arises more and more frequently of how data protection can be guaranteed during this exceptional situation. The concerns regarding infections and paralysis of business are significant. Accordingly, many companies are acting quickly and making important decisions, which, due to the health data of employees, also require an assessment under both European Union (EU) and Luxembourg data protection laws. It is essential to note that violations of the data protection laws cannot be justified, even by the COVID-19 pandemic. Once this crisis is over, the authorities may investigate how data controllers and data processors managed these issues.

This Alert summarizes considerations for Luxembourg companies with respect to data protection.

▸ Does the COVID-19 "state of emergency" override data protection law?

No, on the contrary. Due to the enormous risks of COVID-19, companies will process highly sensitive health data of employees to an increased extent, which will continue to be subject to data protection law. Due to the urgent health risk of COVID-19, companies may justify data processing under Art. 6 and art. 9

Building a better working world

of the EU GDPR (General Data Protection Regulation). Such data processing may not be lawful without such a health risk. However, due to the high level of sensitivity, relevant company processes must be carefully examined in terms of data protection law (including Law of 1 August 2018 on the organization of the Luxembourg National Commission for Data Protection (CNPD) and general regime of data protection) and guidelines issued by the CNPD.

In order to prove the lawfulness of data processing to the CNPD, companies must meet their accountability obligation under Art. 5 (2) GDPR. In particular, decisions with relevance to data protection law must be justified and documented.

▸ Are companies allowed to check employees' temperatures?

The data protection law does not expressly regulate checking employees' temperatures. As per the recent guidelines of the CNPD on processing personal data in the context of a health crisis, companies should refrain from asking their employees (and/or visitors) their body temperature on a regular basis. However, they are allowed to encourage the data subjects to share information regarding their potential exposure to any health risks. In such cases, the identity of the data subject and implemented measures may be recorded.

▸ Can the data protection law conflict with homeworking?

Before allowing employees to work at home (homeworking), companies should double check that homeworking of their employees does not violate contractual obligations with third parties. For example, some commissioned data protection agreements may contain corresponding prohibitions. Violations may ultimately lead to contractual penalties and/or termination of data processing contracts by business partners.

▸ What kind of security measures should companies have in place for homeworking during this period?

If employees process personal data from home, they should also comply with the company's internal technical and organizational measures (TOMs). For example, documents containing personal data must be kept confidential, i.e., out of reach of life partners, children or visitors. It is the duty of every company to inform its employees accordingly and to require them to comply with TOMs.

▸ Are companies allowed to inform their employees about infected colleagues by naming them?

The (even if only company-internal) communication of infected employees by name is an intrusion into the rights of the affected employees and must be carefully assessed in each individual case. On the other hand, major risks for other employees and especially their older family members must also be considered. Failure to mention the risk of infection can indirectly lead to the infection of other individuals, especially older people whose mortality rate is particularly high with COVID-19. These health risks should be considered in data protection assessments. The involvement of data protection officers (or external advisors) and the applicability of the proportionality principle is urgently required. Data minimization should also be considered, as it is of essence to restrict as much as possible the recipients of any special personal data.

▸ Do employees/other individuals have to be informed about data processing concerning COVID-19?

Yes, if companies introduce new data processing activities or adapt existing ones with respect to COVID-19, the data subjects must be informed accordingly.

▸ To what extent must companies adapt their data protection documentation?

The adaptation of the processes due to COVID-19 also entails the updating of the data protection documentation, in particular, the data protection impact assessment (DPIA) and the register of processing activities.

▸ Is it necessary to amend IT contracts?

In individual cases, COVID-19 may lead to an exceptional use of the IT infrastructure (because of homeworking or increased public interest in information). In order to prevent outages of the IT infrastructure, respective IT contracts should be assessed with regard to agreed quantity/quality of the IT infrastructure and, if necessary, renegotiated.

▸ Is the concept of force majeure relevant in the context of COVID-19?

Many contracts contain clauses on "force majeure" according to which performance of obligations may be suspended in the event of epidemics. However, companies should only rely on such clauses after a careful assessment of the

individual case, as there is a high risk that the circumstances in question are not sufficient to suspend performance of obligations. Failure to deliver under a contract may lead to compensation claims of the other party.

Depending on the applicable law and on case-by-case basis, companies may be exempted from performing their obligations or may demand contractual adjustments due to special circumstances of the COVID-19 "state of emergency" even without a contractual clause on "force majeure."

▸ When must companies notify their contractual partners of a delayed or impossible service?

Companies must inform their contractual partners immediately due to the contractual duty of considerateness. If information is communicated in time, supply chains can be optimized, and damage-reducing measures can be taken. Failure to inform may result in damages being claimed as compensation.

▸ Taking action to prepare

In many respects, dealing with COVID-19 cannot be distinguished from dealing with other disease waves such as the annual wave of influenza. However, due to the expected extent and the potential economic and data protection consequences, more far-reaching measures may be necessary.

The data of employees is a valuable asset that must be protected. In this respect, precautions should be taken to ensure that a company can master the data protection and IT law challenges of COVID-19.

Specifically, companies can best respond by the following actions:

- Providing relevant information and complying with the transparency, proportionality and data minimization principles.
- Observing the legal limits and implementing the technical and organizational measures (TOMs) to be observed under data protection law, irrespective of the fact that the risks posed by COVID-19 may justify to some extent unlawful data processing activities.
- Being sensitive to changes in standard processes. In general, every deviation requires an assessment under the data protection law.

For additional information with respect to this Alert, please contact the following:

Ernst & Young Tax Advisory Services S.à r.l., Corporate and Regulatory, Luxembourg City

- Stephen d'Errico stephen.derrico@lu.ey.com
- Laurence Chatenier laurence.chatenier@lu.ey.com
- Raluca Silaghi raluca.silaghi@lu.ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EYG no. 001411-20Gbl

1508-1600216 NY
ED None

ey.com