The European Union's General Data Protection Regulation (GDPR) took effect on May 25, 2018 and has necessitated major compliance efforts by corporations doing business within the EU or (in most cases) processing the personal data of EU employees or customers. However, the GDPR’s effect on corporate internal investigations – both within the EU and abroad – has received much less attention, yet requires considerable planning to avoid problems down the road.

Like the EU Data Protection Directive before it, the GDPR covers a very broad range of personal data: "any information relating to an identified or identifiable natural person." Thus, most of the information obtained during an investigation of EU-based employee communications or documents is affected – everything from emails and IMs to pseudonymized data, which by definition can still be related back to an identified natural person.

The illusion of harmonization

The GDPR for the most part does offer the prospect of greater harmonization of EU privacy requirements because it has direct effect in each EU member state. Unfortunately, for internal investigations, the GDPR establishes only a floor of employee data privacy protection. Each member state is allowed to set higher standards.

Thus, multinationals planning for internal investigations that use the data of EU employees should keep in mind the overall GDPR requirements as well as national laws relating to the GDPR.
What is more, other types of national laws will apply – for example, employment laws, labor laws, blocking statutes, secrecy of correspondence laws, criminal laws and in some cases, laws governing where data may be stored. In other words, employers cannot take the "one stop shop" idea literally when conducting internal investigations involving data of EU personnel.

Territorial scope

The GDPR's extraterritorial reach may come into play even for corporations established outside the EU. In the context of investigation, multinationals will often need to comply with the GDPR if there is any connection to EU data, even if the data being reviewed is (legally) stored outside the EU, eg, on email servers in the US.

Data processing for investigation purposes

GDPR requirements affect investigations even at the earliest stages – for instance, when initial data is being sought. Review, disclosure and/or transfer of personal data, whether to affiliated companies or to IT forensic providers or authorities, must be justified.

In general, no sensitive or private employee or contractor data, such as personal photos, medical appointments or private emails may be collected or reviewed, and this data must be identified and excluded from collection and the review.

The GDPR's basic principles must be followed with regard to processing of personal data:

- processing must take place in a transparent manner; concretely, this may mean providing specific notice to custodians that their data will be processed in connection with an investigation
- processing is limited to what is necessary in relation to the purpose of the investigation; in practice, this implies careful filtering of data before any collection, storage or review is conducted
- appropriate safeguards are followed, and the data is not used beyond the purpose for which it was collected; this may be accomplished by limiting access to investigation data and implementing additional security measures.

At all stages, the company’s data protection officer should be informed and in many jurisdictions, the works council (if any) must be informed or consulted.

Although many companies had relied on consent to support internal investigations, more complex advanced planning is now required. Although in theory, it is possible to request consent of the involved employees, the bar for valid consent has been raised higher under the GDPR. In addition, some national courts have even ruled that, in the context of a corporate internal investigation, an employee cannot give free and valid consent. Thus, it is crucial to determine whether consent is indeed required, and why. For example, the risk of criminal law violations may justify reliance on consent, but not for the purpose of the GDPR, absent related national law requiring consent.

Data transfer

The GDPR requires that any transfer of data to a third party located outside the EU – even within a corporate group, for instance when the compliance/investigation team sits within another group entity outside the EU – satisfy specific conditions.

The GDPR's rules regarding international transfer are essentially similar to those provided under the 1995 Directive, with a couple important changes. For example, while the data protection supervisory authorities' authorization to transfer data pursuant to so-called 'model clauses' is no longer required, transfers that are not made by an EU controller will still require authorization.

Regarding transfer of data to the US, the EU/US Privacy Shield thus far offers participating corporations a way to transfer investigation data, eg, to a group corporation in the US.

Finally, much attention has been paid to GDPR Article 48, which states that a transfer requested by an administrative authority outside the EU is enforceable where it is based on international agreements, such as mutual legal assistance treaties. In many investigations, a thorough assessment is required to understand how to strike the proper balance between compliance with the GDPR and other applicable EU laws, and cooperation with the requesting authorities.
Sanctions

Famously, the GDPR could in theory bring very serious sanctions for businesses, including revenue-based fines of up to €20 million or 4 percent of annual worldwide turnover.

Although the maximum fines are very unlikely to be imposed for minor non-compliance in justified investigations, the new regime will significantly increase risk exposure. This goes along with the fact that all the EU data protection supervisory authorities also now enjoy wide investigation and corrective powers.

We believe that in the future we will see a number of cases alleging GDPR violations during an internal investigation. It is easy to foresee that affected employees could allege an investigation is not in compliance with the GDPR and will inform the supervisory authorities.

In addition, the GDPR also provides that a person who suffers material or non-material damage as a result of a violation of the GDPR has the right to claim compensation.

Conclusions

Prudent businesses will review existing internal investigation guidelines and policies and, if applicable, works council agreements, and revise them to reflect GDPR requirements and those of other applicable laws. In some jurisdictions, investigation procedures can be agreed upon in advance with the works council in order to comply with the GDPR and other applicable national laws.

The GDPR's accountability requirement means that during an investigation, every decision must be documented. Should authorities outside the EU be involved in an investigation, it is critical to make clear to them from the start the data protection limitations set out by the GDPR and other applicable laws.

For more on the implications of the GDPR on investigations, please contact the authors. General information about the GDPR and what it means for your company can be found in the DLA Piper General Data Protection Regulation Guide.

AUTHORS

Jim Halpert
Partner
Washington, DC | T: +1 202 799 4000
jim.halpert@dlapiper.com

Dr Daniel Zapf
Counsel
Frankfurt | T: +49 69 27133 0
Daniel.Zapf@dlapiper.com

Carol A. F. Umhoefer
Partner
Miami | T: +1 305 423 8500
carol.umhoefer@dlapiper.com