The GDPR introduces new notification rules for personal data breaches: What you need to know

02 July 2018

With the General Data Protection Regulation (GDPR) now in force, the focus on privacy and data protection throughout the European Union (EU) is stronger than ever before. With this new law comes new obligations for companies to comply with an EU-wide notification regime when a breach of personal data occurs.

The GDPR and European regulators provide detailed guidance on which personal data breaches must be reported to regulators and when, as well as when notifications are not needed. Reports must be made to different individuals in different cases; for example, if the breach is likely to cause a risk to the rights and freedoms of an individual, the lead data protection authority must be notified. If the breach results in a high risk to the rights and freedoms of an individual, the individuals affected by the breach must also be notified.

In this hoganlovells.com interview, Joke Bodewits, counsel in the Hogan Lovells Amsterdam office, provides a comprehensive overview of the GDPR's reporting requirements regarding breaches of personal data, and she offers recommendations for identifying and investigating these so-called personal data breaches.

How does the GDPR define personal data, and how will data breach reporting requirements be enforced?

Joke Bodewits: The GDPR is relevant when personal data is involved, and "personal data" means all data that can directly or indirectly identify a natural living person, including names, e-mail addresses, ID numbers, credit card numbers, and online profiles. Under European law, it doesn't matter if it relates to an individual acting for private or for business purposes.

For noncompliance with the breach notification obligations, administrative fines can be imposed up to €10 million, or two percent of your global annual turnover. It may seem like a softer regime than the €20 million or four percent that applies to a breach of the basic principles of the GDPR, but don't be surprised, because it may end up as a double administrative fine in practice. This means that you can receive a two percent fine for failing to comply with breach notification obligations. In addition, you can receive a two percent fine based on your failure to implement appropriate security measures.

The breach notification requirements set out in the GDPR are directed at data controllers, which are obliged to notify data breaches with data protection authorities that have an impact on a person's private life. The breach notification requirements furthermore require data controllers to notify data breaches to affected individuals if the data breach is likely to result in a high risk to the rights and freedoms of the individual. If such personal data breaches take place, notifications should be made without undue delay. This rule is quite similar to what we have had in the Netherlands since 2016, but it is new in most countries in Europe.

How does the GDPR define a breach of personal data?

Bodewits: The GDPR provides a very broad definition of personal data breaches. It can relate, for instance, to the accidental or unlawful destruction of personal data, such as the deletion of records or technical errors that result in the deletion of data. Loss of personal data can also be the result of encryption by ransomware, or because you lost the passwords. The loss of data can be permanent or temporary; in both instances, it is a personal data breach.

A breach can also relate to the unauthorized access to or disclosure of personal data. For instance, if unauthorized employees have access to personal data or if an e-mail with personal data is sent to the wrong recipient.

How do you know if you have a reportable breach? And when is the notification requirement triggered?

Bodewits: The GDPR notification obligations do not include data breaches where no personal data is affected. So if you only talk about a security incident, that is not directly considered a personal data breach. However, if personal data is affected and is likely to have an impact on a person's private life, those breaches should be notified without undue delay, and in no event later than 72 hours after the company becomes aware of it.

"Becoming aware" means that you must have a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. When, exactly, a data controller can be considered to be "aware" of a particular breach will depend on the circumstances of the specific breach. In some cases, it will be relatively easy to determine that a personal data breach has occurred. For instance, if you receive a notification of an incorrectly sent e-mail containing personal data, or a device is reported stolen to an IT department, or you're contacted by a processor about a potential security incident, these are all situations where an awareness of a personal data breach can be created. In other cases, it may take some time to establish if personal data has been compromised. In such events the emphasis should be on prompt action to investigate the incident to determine if personal data has indeed been compromised, and if so, to take remedial action and notify if required.

What is important is that all information regarding a potential breach is taken seriously and

investigated. So it's important that as soon as you receive information about a potential breach — for instance, if the breach took place with a processor — you immediately reach out to your processor and ask questions about the breach, such as what happened? Which personal data was compromised? Which individuals could be affected? Which measures have been taken to mitigate the negative consequences of the breach? Why hasn't the breach been reported by the processor? How to prevent this from happening again?

Considering that most data controllers depend on the information sent by their data processors, it is important to include in data processing agreements that processors are obliged to cooperate and provide all reasonable assistance in the event of a personal data breach. When you receive information about the breach, emphasis should be on investigating the breach and taking mitigating actions within that 72-hour timeframe.

Data protection authorities acknowledge that 72 hours is a short period of time, but they believe that if companies prepare for personal data breaches, plan for likely scenarios such as phishing incidents, and create incident response plans, they will be able to meet this deadline.

When conducting internal investigations of breaches, what should companies consider?

Bodewits: They should consider the scope and nature of the personal data breach, meaning they should — amongst others — assess the type of breach, sensitivity of the data, amount of personal data, and ease of identification. You also have to consider the likely consequences of the breach — meaning *all* consequences of the breach, from financial consequences to stigmatization, exclusion, fraud, identity theft, or just inconvenience. Then you should consider the actions you should take to mitigate the likely consequences of the breach. If you have the ability to remotely wipe data, this is an exercise that could mitigate the consequences and may even eliminate notification requirements.

You can also consider using a forensic investigator to help you conduct an internal investigation to see whether a breach actually is a personal data breach. We know from experience that those companies can usually investigate and inform you within two or three days about the scope and nature of the breach, whether it is a personal data breach, and the potential consequences such breach can have on the private lives of the affected individuals. What's very important is that you work together with your internal breach response team to make sure that you are as effective as possible, that you take it all seriously, and make sure that you document what you do and why you do it.

The findings of the internal investigation should ultimately be reported to data protection authorities if you have a reporting obligation. If these findings do not reveal all relevant aspects of the notification obligation, EU regulators state that this should not be a reason for not notifying in time. The focus should be on addressing the adverse effects and meeting

notification obligations, and not so much about having accurate figures in your notification — as the notification can be amended or withdrawn at any time.

What format should companies use for notifying authorities of a personal data breach?

Bodewits: EU regulators issued guidance in February 2018 stating that submitting a general notification in time is an arguable approach, as notifications can be amended or withdrawn at any time. Also, in the event of a series of incidents, EU regulators have stated that you can combine those incidents into one bundled approach.

It is important to know that there is no standard template or breach notification form that you can use for all European data protection authorities. The notification form and language requirements may vary from country to country. Companies should check with the relevant data protection authority when the notification is made as to what form the notification should take. For instance, in the Netherlands, all notifications must be made online, in Dutch, using the regulator's notification form. Similar rules may apply in various jurisdictions in Europe. If a breach affects multiple entities in Europe, the data controller should notify the lead data protection authority. If the company is not established in Europe, notification should be made with the data protection authority in the country where the EU representative is established.

Under what circumstances are notifications not required?

Bodewits: If the investigation shows that it is unlikely that the breach will have an impact on the private life of the affected individuals, no breach notification is required. For instance, if only the first names and hashed e-mail addresses of the individuals are affected by the breach, if the data is encrypted, or if a stolen device is remotely wiped, in all those instances you could say that there is no impact on the private life of the individuals and therefore, it is not necessary to notify the regulators.

This should be assessed on a case-by-case basis. The assessment should concern all the relevant aspects of the case. For instance, if a database with marketing e-mail subscribers is temporarily unavailable due to a loss of power, this will not impact the private life of an individual. But this is different when it concerns medical records in a hospital. Even if the breach is not reportable to data protection authorities or affected individuals under EU laws, it should always be registered internally. We recommend that you keep an internal register containing the data you would normally provide to an EU regulator, so you have an overview of the investigations you conducted and findings and remedial actions in relation to the personal data breach.

There is one important thing to add: some data protection authorities, such as in the Netherlands, allow for anonymous incident reporting by employees, customers, or the media — if there is a fear that the data controller has not or will not notify the data breach itself.

Anonymous reports are investigated in detail by data protection authorities and have resulted in compliance investigations. Since the GDPR has entered into force, the Netherlands regulators have daily received about 25-30 notifications about how companies handle personal data, including anonymous breach reports, and authorities are very active in investigating them. For the United States, it's good to know that if any employees are concerned with making anonymous reports, they are protected by the whistle-blowing rules in many European countries.

In addition to the breach notifications to authorities mandated by the GDPR, there are also notifications that apply to affected individuals. Please explain.

Bodewits: Notifications apply when there is a high risk to the private life of the affected individual. It can be assumed that if the personal data breach affects financial data, sensitive data, or data that could result in identity theft, stigmatization, or exclusion, it is considered a personal data breach that should be notified to the affected individuals.

All communications to individuals should be clear and comprehensive. This means that individuals should understand what it says and what they can do themselves to mitigate the consequences. In some countries, a copy of the communications must be provided to the data protection authority, and therefore it is very important to align the facts you provide to the individual with the facts you provide to the data protection authority. It's also important to think about the way you want to communicate the breach, as the communication could attract unwanted media or other attention.

Are there instances when notifying individuals is not required?

Bodewits: Yes — notification is not required if the affected data cannot be used by the recipient because it is encrypted or remotely wiped, or if the risk is unlikely to materialize because the data controller has taken technical or organizational measures such as blocking access to personal data or improving security measures. Lastly, notification is not required if it would require a disproportionate effort. For instance, if the data controller has no knowledge that it affected individuals because the data is permanently lost and no back-up data is available. Arguing that it is disproportionate is very difficult, however, so this is a last resort only.

The data controller may use the regulator notification to wait for the regulator's instructions as to whether notification is required. We recommend, however, making internal assessments to determine this instead of asking a data protection authority to do this for you.

About Joke Bodewits

When clients need business-focused, pragmatic advice for using and protecting data, they turn to Joke Bodewits. She understands the legal needs of her clients. As a problem-solving advocate,

she sees the connections between law and business realities and helps clients resolve compliance and enforcement problems with practical solutions and minimal corporate pain.

Contacts

Joke Bodewits
Partner

> Read the full article online