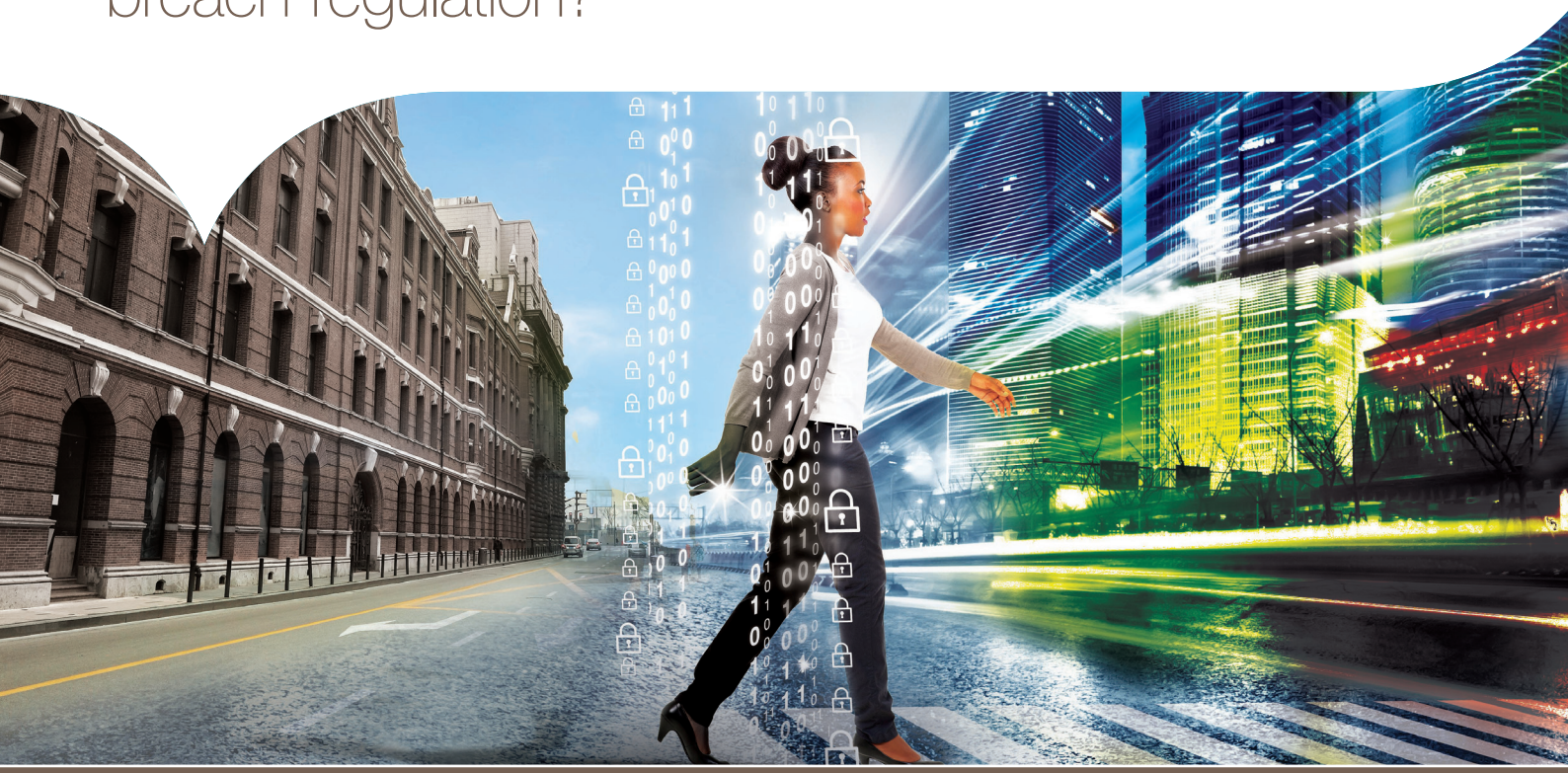
Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Capgemini Consulting

Are you ready to adapt to the changing data breach regulation?



Mandatory Dutch data breach notification for all industries with increased regulatory fines in force by 1 January 2016.

Mandatory data breach notification: stricter laws, bigger penalties

The Dutch First Chamber passed the general[1] Bill on Data Breach Notifications, which requires mandatory notification of privacy and security breaches of personal data for all companies (data controller) in the Netherlands. At the same time, the sanctions for violating the new bill (and the Dutch Data Protection Act in general) have increased significantly.

In the event of a data breach, the Dutch data protection authority needs to be notified immediately. Additionally, the individual data subjects, whose personal data are compromised, need to be informed if the data breach has any adverse consequences to their private life.

Failures to notify are subject to the recently increased fine of a maximum of EUR 820.000 or 10% of the company's annual net turnover per violation.[2]

The Dutch data protection authority (Autoriteit Persoonsgegevens) has started enforcement of the new Data Breach Notifications Bill by 1 January 2016.

International scope of data breach notification

The changes in the Dutch data protection act are the harbinger of the upcoming European Data Protection Regulation, which will be enacted during the first half of 2016. After an implementation period of two years, the European directive will be enforced by the national DPA's.[3]

The European directive aims to harmonize the various national data protection regimes. Data breach notification requirements and sanctions will be further increased and will be subject to the company's global turnover.

Reporting data breach is a corporate social responsibility

Besides the binding legal obligation to notify data protection authorities and data subjects, reporting on data breaches has also become the status-quo in external corporate responsibility statements. The Global Reporting Initiative (GRI) sustainability standard contains a performance indicator reporting the total number of substantiated complaints regarding breaches of customer privacy and losses of customer data.[4]

With thousands of reporters in over 90 countries, GRI provides the world's most widely used standards on sustainability reporting and disclosure, enabling businesses, governments, civil society, and citizens to make better decisions based on information that matters. 93% of the world's largest 250 corporations report on their sustainability performance.

Avoid regulatory fines and reputation damage

As stated above, incorrect or delayed data breach notifications are subject to fines up to EUR 820,000 or 10% of the company's annual net turnover per violation.

Having a good data breach notification in place reduces the risk of regulatory fine significantly. As the timelines of notification are very tight[5], procedures and systems need be in place in advance to support companies notifying customers and regulators appropriately in the event of a data breach.

Thoughtful reporting of data breaches in corporate sustainability annual reports increases the company reputation as reliable treasurer of personal data.

Not reporting on customer privacy indicators is no longer an option and will automatically lead to two dreadful conclusions: namely, that the company has no data breach notification process in place, or that the company has some breaches to hide. Both of these assumptions are open invitations towards the enforcement authorities. None of them is desirable for a reputed company.

Put your data breach process in place now

A well implemented data breach process is crucial for timely and accurate notification. Incident response processes have to be implemented and procedures have to be in place to facilitate the notification process. Furthermore, every single employee has to be aware to identify possible data breaches and the internal reporting procedures that need to be followed.

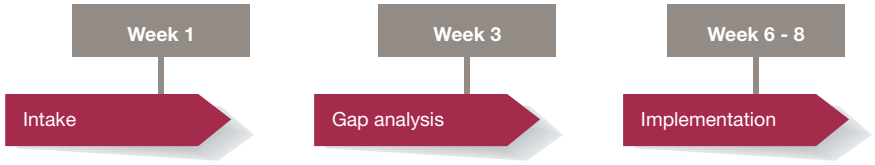
Companies are advised to make appropriate changes to their data privacy policies, revise their existing data compliance process frameworks, and to invest in the awareness of their employees to avoid any data breach sanctions. Moreover, decision governance mechanisms have to be in place to judge if customers need to be informed about a data breach.

Rely on proven masters implementing the data breach process

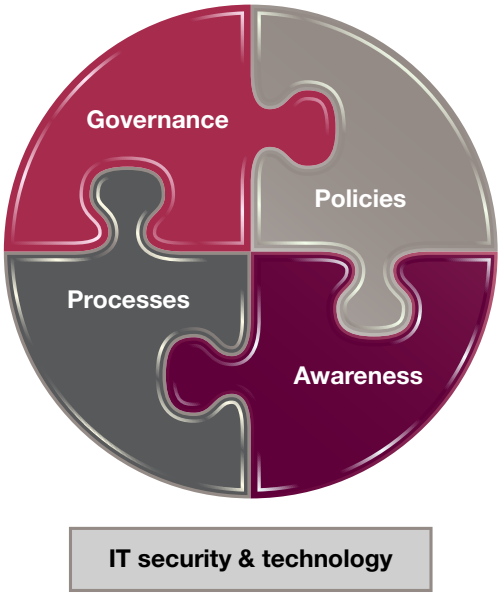
Capgemini Consulting brings the expertise, experience, business insight, tools, and proven solution components to maximize success in your journey to implement the data breach notification process. We have already done so for companies across all sectors and industries. Data Breach Notification Governance is part of our Privacy-in-Control proposition that has been delivered to numerous renowned companies.

The implementation effort of a data breach notification process depends on the current situation, complexity, and size of a company. On an average, the implementation lead-times vary between six to eight weeks. In situations where companies have a particular large number of subsidiaries or local outlets, the implementation effort and lead-time might be higher.

Data breach notification implementation process of Capgemini Consulting



Capgemini Consulting Privacy-in-Control approach



Glossary of terms

Data controller
A body (either alone or jointly or in common with other persons) who determines the purposes for which and the manner in which any personal data are or will be processed.

Data subject
An individual who is the subject of personal data, i.e. the person whose data is, or will be, processed.

Data Protection Authority (DPA)
National regulator enforcing the data breach notification bill. In the Netherlands this role is fulfilled by the Autoriteit Persoonsgegevens.

Global Reporting Initiative (GRI)
GRI is the world's most widely used standards on sustainability reporting and disclosure, enabling businesses, governments, civil society and citizens.

Measure once, leverage thrice!

The unique Capgemini Consulting approach maximizes the benefit of your data breach notification efforts. While the detection of data breaches needs to be implemented only once, the obtained information can be used in threefold:

1. Timely notification of data protection authority to avoid sanctions,
2. Managing the customer relationship by informing the subjects whose data had been compromised, and
3. Increasing trustworthiness and credibility of the company by reporting on data privacy in the external sustainability statements.

Data breach prevention needs a holistic approach

The aim of every company should be to avoid any kind of data breach incidents. However, whenever such an undesirable event occurs, a well implemented notification process is imperative to provide an appropriate response.
The Capgemini Consulting Privacy-in-Control approach helps companies to put effective prevention mechanisms in place by implementing a comprehensive privacy compliance framework. Our approach covers the various dimensions of privacy governance, risk management, policies, processes, information technology, and employee awareness.

[1] Data breach notification has earlier already been adapted in the telecommunication industry (enacted by 5 June 2012 as part of the Dutch Telecommunications act)

[2] Data protection regime beefed up: higher sanctions and mandatory data breach notification, De Brauw Blackstone Westbroek, 28 May 2015, http://www.debrauw.com/alert/data-protection-regime-beefed-higher-sanctions-mandatory-data-breach-notification

[3] EU states agree framework for pan-European data privacy rules, The Guardian, June 15, 2015 http://www.theguardian.com/technology/2015/jun/15/eu-privacy-laws-data-regulations

[4] GRI's G3.1 Sustainability Reporting Framework online. https://www.globalreporting.org/standards/G3andG3-1/guidelines-online/G31Online/StandardDisclosures/ProductResponsibility/Pages/PR8IndicatorProtocol.aspx

[5] Timelines of reporting will be clarified by DPA. The telecommunication breach notification bill requires immediate (onverwijld) notification to the authorities. The regulator hotline (Loket Meldplicht Telecomwet) is available 24/7. https://www.meldplichttelecomwet.nl/

Contacts

Erik Hoorweg
Vice President
erik.hoorweg@capgemini.com
Tel: +31 6 1503 0869

Andre Walter
Managing Consultant
andre.walter@capgemini.com
Tel: +31 6 5541 5810

Capgemini Cybersecurity team
cybersecurity.bnl@capgemini.com

About Capgemini

Now with 180,000 people in over 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2014 global revenues of EUR 10.573 billion.

Together with its clients, Capgemini creates and delivers business, technology and digital solutions that fit their needs, enabling them to achieve innovation and competitiveness.

A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Learn more about us at
www.nl.capgemini.com

Rightshore® is a trademark belonging to Capgemini

About Capgemini Consulting

Capgemini Consulting is the global strategy and transformation consulting organization of the Capgemini Group, specializing in advising and supporting enterprises in significant transformation, from innovative strategy to execution and with an unstinting focus on results. With the new digital economy creating significant disruptions and opportunities, our global team of over 3,600 talented individuals work with leading companies and governments to master Digital Transformation, drawing on our understanding of the digital economy and our leadership in business transformation and organizational change.

Find out more at:
www.capgemini-consulting.nl

Capgemini Nederland B.V.
Reykjavikplein 1
P. O. Box 2575, 3500 GN Utrecht
Tel. + 31 30 689 00 00

IN/1B-009.16a