

Privacy as a Business Enabler



Telecommunication industry perspectives

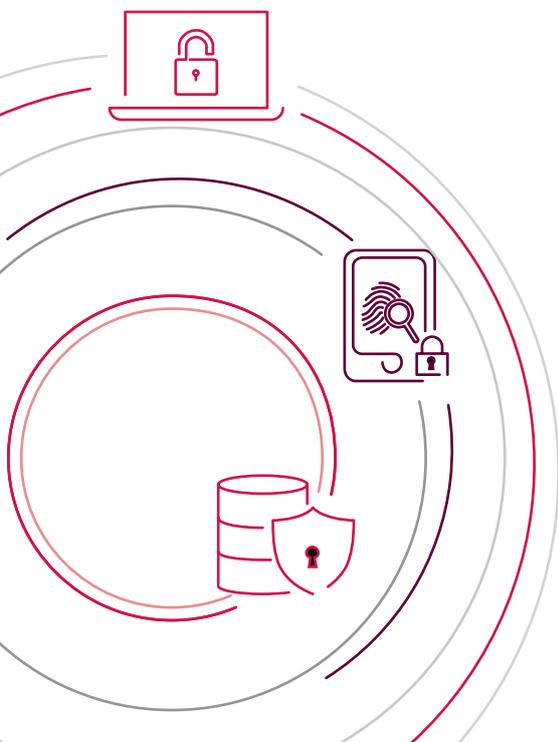
Capgemini understands that besides process and technology, concepts focusing on human aspects are an essential part of the business equation. By helping companies to comply with consumer expectations, we make privacy a differentiator for their business strategy.

Accountability, trust and individual freedom are cornerstones in the concept of privacy. They are also rooted in the value system of Capgemini.

Collaboration with our customers is central to the way we do business. Collaboration with end-consumers on the topic of privacy is crucial in an environment where non-tangible assets (such as brand reputation, customer experience, trustworthiness and corporate responsibility) are increasingly becoming key differentiators.

Capgemini aims to empower your organization to respond quickly and appropriately to these changing market demands.

Capgemini will help you to draft a unique, collaborative privacy framework based on your propositions, geographical footprint, and your position in the value chain. As a global IT leader with our roots in applications and business transformation for more than four decades, we can not only help you to deliver this framework, but also make it work for you.



The telecom market situation

Non-tangible assets such as customer experience, trust, brand value, reputation, and corporate responsibility have become the new differentiators. At the same time, mobile communication markets are under serious pressure. We see a tendency in European markets for traditional service revenues to stagnate and even decline.

Saturation of the market is caused by various factors, including shift from traditional voice and texting services to mobile data, changes in roaming regulations and Wi-Fi offload. Increasingly, Over-the-top (OTT) players like Skype, Google and Apple are entering the competitive arena.

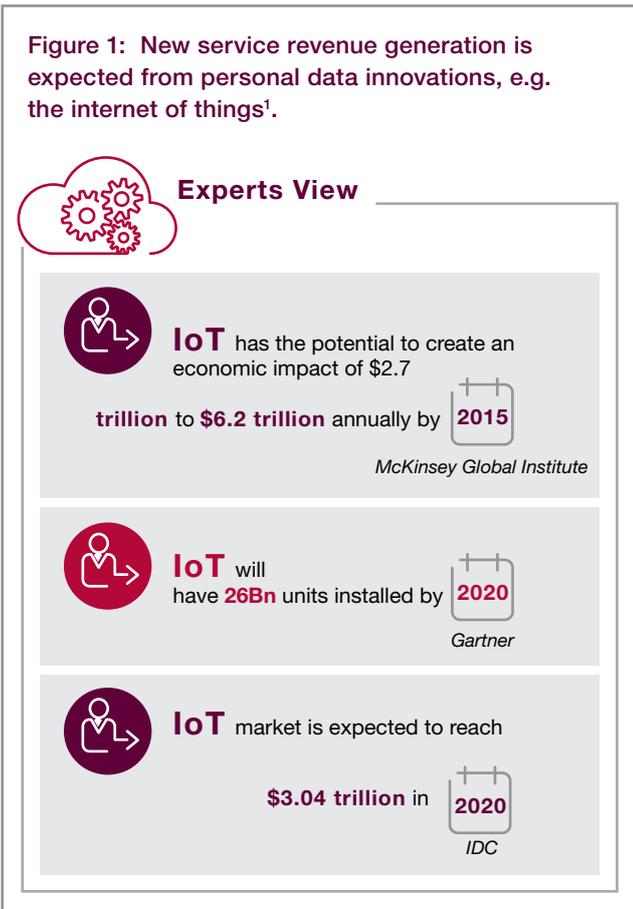
New service revenue generation is expected from personal data innovations in the area of mobile advertising, mobile payment, value added services, internet of things and big data initiatives in the broader sense.

At the same time regulators, both at national and European level, are tightening the privacy and data protection regulations. Compared to the US, there are stringent regulations in place in Europe that restrict service providers in the ways and extent to which they can make use of consumer data.

“ Facial-Recognition Concerns Keep Facebook ‘Moments’ From Europe.”

Beside this, consumers demand more transparency and autonomy when it comes to processing their own personal data. An emerging trend can be seen in the so called (corporate) Personal Information Management Systems³. These solutions aim to put individuals in control of their own data.

Figure 1: New service revenue generation is expected from personal data innovations, e.g. the internet of things¹.



Personal Information Management System (PIMS) initiatives start-up all across Europe. Examples are: Qiy⁴ (Netherlands), MyData⁵ (Finland) and Mydex⁶ (UK)

A future-proof privacy strategy as a building block for consumer trust

The demand for more control over personal data puts new business models on the horizon, where the value of data is put in the hand of the consumer. You should ask yourself the question: is my business prepared for a future where consumers, not companies, call the shots on personal data?

Businesses must recognize privacy as part of their product and service strategy. Firms with privacy-friendly business models and service architectures will differentiate from their competitors.

A future-proof privacy strategy is a competitive advantage in the age of the consumer. Trust and the economic value of the personal data assets are intertwined.

Consumers will become increasingly aware of the tradeoff between relevant services, richer and better experience, and their privacy. A modern privacy strategy is not just about protecting the consumer data, it must enable consumers to be in control of this tradeoff.

Increased consumer trust will encourage the willingness to share data with the businesses. This will bring a plethora of benefits: consumers will have access to a richer set of services with greater experience and companies will have access to consumer data to accelerate this trend. Telecom business will be enabled to tap into newer revenue streams.

Successful data-driven opportunities

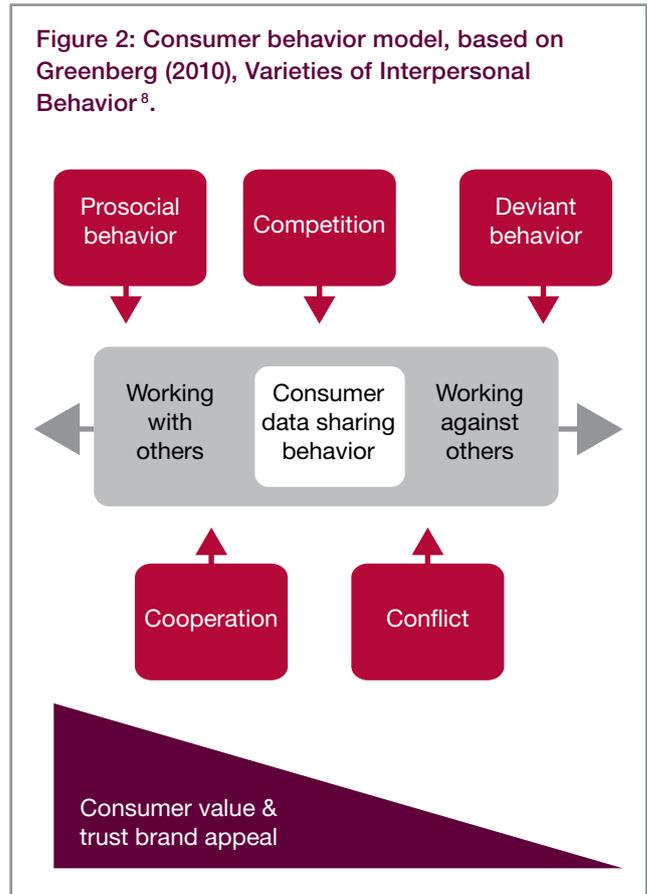
The consumer data sharing behavior is crucial for the success of future (big) data initiatives. The consumers' willingness to provide personal data depends on the level of trust in the company that collects and uses it.⁷

The more data consumers are willing to share, the more value can be created. Be aware, the opposite can also happen: opportunities for the digital economy are at risk if consumers refuse to share information.

In this digital era, the consumer becomes an integral part of the organizations. Traditional models from organizational behavior⁸ helps us to understand the consumer data sharing behavior, see figure 2.

Higher trustworthiness and brand appeal of companies positively influence consumers' willingness to share data.

The table below shows some examples of observed consumer data sharing behaviors.



Level	Observed Data Sharing Behavior
Prosocial Behavior	Participate in open data, voluntary data sharing, “donating” data, gratuitous positive posting on social media
Cooperation	Proactive data sharing, product reviews, forums, co-development
Competition	Negotiate data exchange, cookie acceptance, etc.-> value exchange is expected (e.g. share data to use free services, improve service experience, etc.)
Conflict	Complaints about personal information processing, legal or regulatory litigation, negative press
Deviant Behavior	Hacking, Consumer activism, including Ad-Blocking, Profiling Sabotage ⁹ , Fake Identities ¹⁰ , Abuse of Personal Information Request Engines ¹¹

Obviously, all companies seek for cooperative or even pro-socially behaving consumer. This calls for consumer trust, together with the ability to create added value for the consumer.

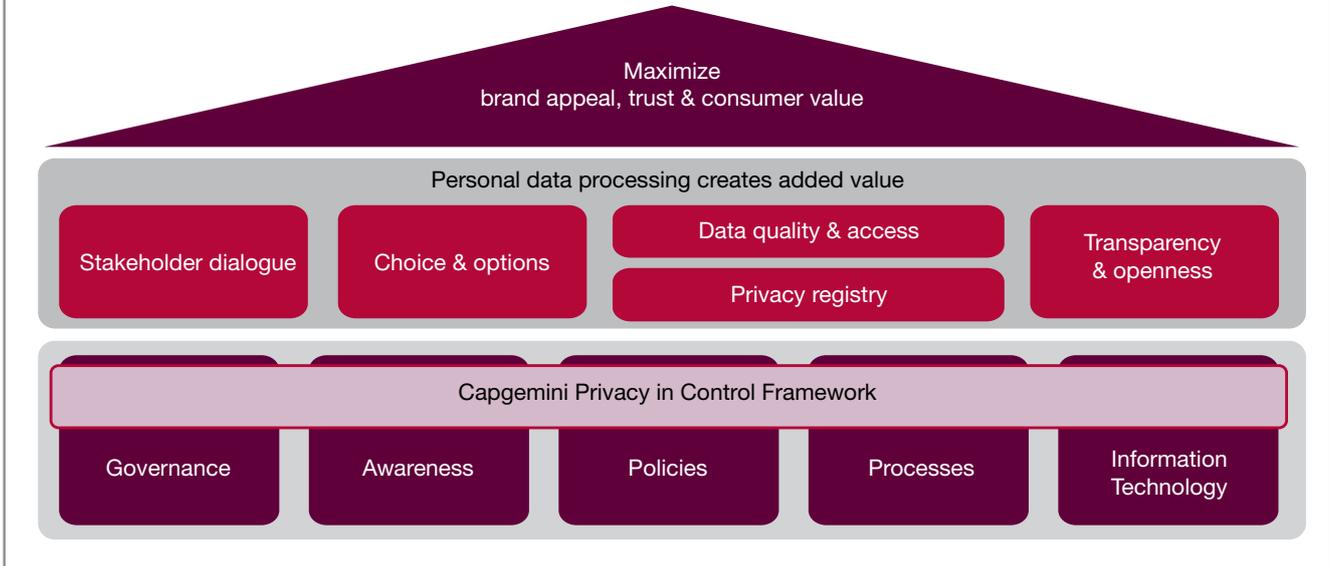
More than half of the people today view their personal information as an asset to be used to negotiate better deals with brands, a UK report says.¹²

No company wants to end up in a situation where consumers show conflicting or deviant behavior. The estimated loss of

global revenue due to ad-blocking alone is more than 20 billion USD during 2015.¹³

81% of people between 18-24 years admit to provide wrong information when asked for personal information. 73 % believed the risks outweigh the benefits when handing over data.¹⁴

Figure 3: The Capgemini Consulting Collaborative Privacy Model.



What is the best approach to generate trust and create consumer value?

Recent research shows that only 4% of the EU citizens fully trust telecommunication and internet providers. Another 29% partially trusts them.⁷

The Capgemini Consulting approach is focused on increasing consumers’ trust levels. We apply our trust formula, which considers the influences of consumer intimacy, credibility, and the risk appetite of the data collecting company.

Based on this, Capgemini Consulting has developed the Collaborative Privacy Model to foster consumer trust in personal data economies, see figure 3.

The Capgemini Consulting Collaborative Privacy Model helps to increase 1) consumer intimacy, 2) your company’s privacy credibility, and 3) reduces your privacy risks effectively.

$$\text{TRUST} = \frac{\text{INTIMACY} + \text{CREDIBILITY}}{\text{RISK}}$$

Consumer intimacy

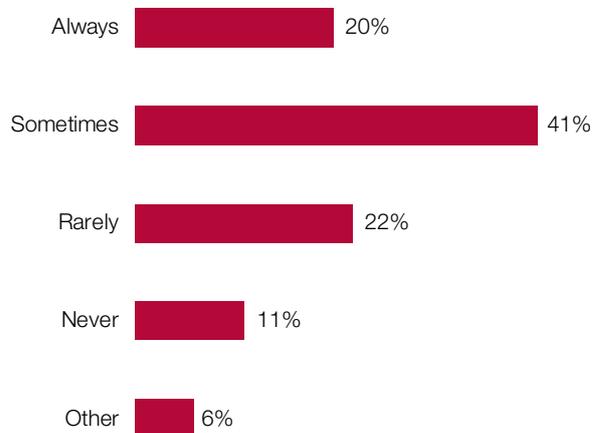
Consumer intimacy is stimulated by engaging in stakeholder dialogue, openness, and transparency. These capabilities are the key ingredients for building accountability and trust, which are necessary for the functioning of data economies.¹⁵

Stakeholder Dialogue: Enter into a dialogue with your consumers and other stakeholders about the expectations they have towards your company collecting and using personal data.

Openness: Be open and honest about the purpose of processing personal data. Communicate your privacy commitments clearly to all stakeholders, and live up to it.

Transparency: Inform consumers about how your company processes personal data in a clear and understandable way. Stakeholders need to understand clearly how you take responsibility to comply with privacy regulations and public expectations.

Figure 4: “Only 20% of the respondents are always informed about data collection and the way data is used”¹⁶.



Privacy credibility

Your company's credibility is strengthened by demonstrating your privacy expertise, your ability to give consumers a voice in the data sharing process, and the quality of the consumer data you hold.

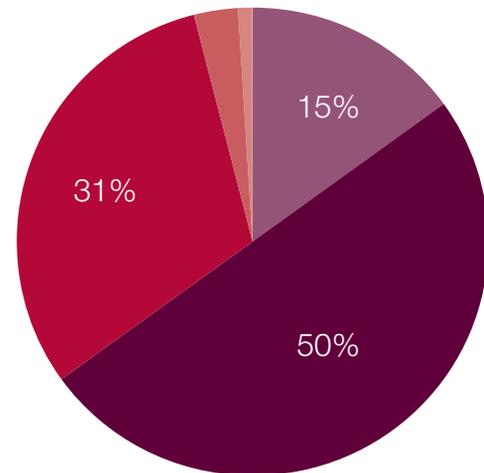
Privacy Expertise: Develop and demonstrate your privacy proficiency. Consumers expect you to be on top of the privacy regulations and public expectations.

Data Quality: Consumer data needs to be accurate, authentic, accessible, and up-to-date to enable your company to develop relevant offers and propositions. Among others, this requires a well implemented data ownership, governance, and operational life cycle.

Choice & Options: Genuine consumer consent is a very powerful legitimacy of processing personal data. Support your consumers to understand their data sharing benefits, so that they can make informed and conscious choices of sharing their data.

Privacy Registry: Provide a single point of truth of the consumers' personal data settings and transactions. Provide insights on consumer profiling, permissions that have been given, and with whom their data has been shared.

Figure 5: "Two-thirds of respondents (67%) are concerned about not having complete control over the information they provide online."¹⁶



- Complete control
- Partial control
- No control at all
- It depends on the website or application (SPONTANEOUS)
- Don't know



Risk reduction and compliance

Risk reduction and compliance are the foundation of the Collaborative Privacy Model. This is achieved by implementing a mature and effective privacy compliance framework. Privacy certifications¹⁷ can underline and demonstrate the compliance statement.

The Capgemini Privacy in Control framework (figure 3) sets out the privacy governance and implements the privacy policies into the company processes, systems and hearts and minds of their employees. It is particularly important to be prepared for the increasing accountability obligations and financial penalties introduced by the new European General Data Protection Regulation¹⁸

Governance: Clarify ownership and accountability of privacy compliance, risk management, and decision-making. Facilitate internal and external privacy assessments, audits and reporting.

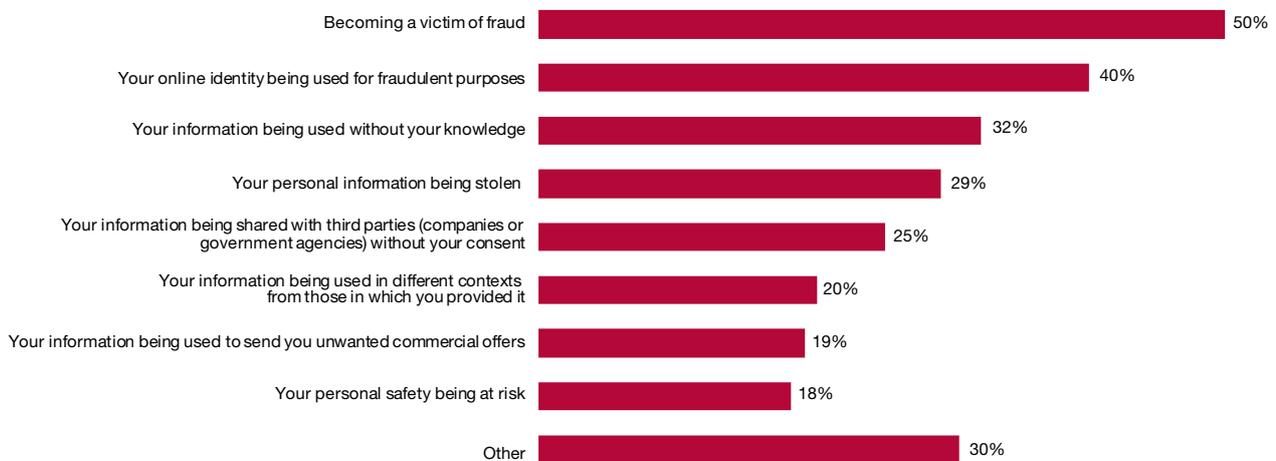
Policies: Formulate legal, compliance and consumer privacy policies that outline the principles, values, standards and rules of behavior expected.

Processes: Implement privacy-specific processes (e.g. data breach notification) and embed privacy controls in the business processes. It is important to measure operational privacy performance.

Information Technology & Security: Implement adequate information security measures and controls (e.g. identity and access management). Create data inventory of all systems that hold personal data.

Awareness: Develop training and awareness material to make privacy top of mind (e.g. Privacy e-learning). Support in internal and external communication plans on privacy.

Figure 6: “Half of the respondents say that becoming a victim of fraud is the most serious risk associated with their personal information”¹⁶.



Creating consumer value

Creating consumer value requires insights on what truly delights your customers. Exciting services, convenience, great user-experiences or monetary benefits, to name a few, can make the difference.

The challenge, however, is to develop sustainable data strategies that encourage consumers to share their information, to convince them to opt-in for your services and to reinforce their engagement.

For example: WEVE, a UK based mobile marketing company (at the time of the case a joint venture of O2, Vodafone and EE), increased the awareness of Pizza Hut's various promotions like happy-hour. This was done through advertisements across multiple channels, delivering a series of highly targeted mobile messages to specific audiences at particular times of the day close to Pizza Hut restaurants. The result: mobile became the best performing channel for driving sales.

Being able to make consumers understand the benefits of sharing their preferences, location, and so forth, WEVE was able to accumulate 17 million opt-ins within a period of 8 months.¹⁹

Conclusion

Telco's are well positioned to take the lead in personalized services, but they need to act now. Consumer willingness to share personal data is crucial for the success of future data-driven opportunities. Success highly depends on the level of trust in the data collecting company. Moreover, it is essential that sharing personal details must create perceived value for consumers.

Capgemini Consulting applies the collaborative privacy approach to leverage trust in your company, improve brand reputation, and help you to develop and implement sustainable, consumer value creating privacy strategies.



For more information please contact

Andre Walter

Author & Privacy Consultant
Capgemini Consulting
andre.walter@capgemini.com
Tel: +31 6 5541 5810

Erik Hoorweg

Vice President Cybersecurity
Capgemini Consulting
erik.hoorweg@capgemini.com
Tel: +31 6 1503 0869

Han Michels

Vice President Telcom, Media & Entertainment
Capgemini Consulting
han.michels@capgemini.com
Tel: +31 6 2715 9295

Referenced sources and footnotes

1. Experts view on the potential of the internet of things http://www.slideshare.net/intelligentia_IT/internet-of-things-facts-and-stats
2. WSJ - Facial-Recognition Concerns Keep Facebook 'Moments' From Europe <http://blogs.wsj.com/digits/2015/06/18/facial-recognition-concerns-keep-facebook-moments-from-europe/>
3. Forrester also uses the term Personal Identity and Data Management systems. <https://www.forrester.com/Personal+Identity+And+Data+Management/fulltext/-/E-RES60322>
4. Qiy- Connecting consumers and organizations to a Trust Framework allows exchange of validated data - <https://www.qiyfoundation.org>
5. MyData – Finish Ministry of Transport and Communications <http://www.lvm.fi/publication/4440204/mydata-a-nordic-model-for-human-centered-personal-data-management-and-processing>
6. Mydex enables individuals to exchange personal data with confidence - <https://mydex.org/>
7. The commercial use of consumer data - Report on the CMA's call for information, June 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/398283/Consumer_Data_-_CFI.pdf
8. Greenberg, J. (2010), Managing Behavior in Organizations, 5th edition, pg.193, Pearson, Boston
9. AdNauseam quietly clicks every blocked ad, data gathered shows an omnivorous click-stream, user profiling, targeting and surveillance becomes futile. <https://dhowe.github.io/AdNauseam/>
10. Fake Name Generator <http://nl.fakenamegenerator.com/gen-random-nl-nl.php> or, Get Creditcard Number <http://www.getcreditcardnumbers.com/>
11. Bits-of-Freedom – Portal for Personal Information Request <https://pim.bof.nl/>
12. Data Privacy: What the consumer really thinks, DMA, UK, 2015, http://www.dma.org.uk/uploads/ckeditor/Data-privacy-2015-what-consumers-really-thinks_final.pdf
13. The cost of ad blocking, PageFair and Adobe 2015 Ad Blocking Report, http://downloads.pagefair.com/reports/2015_report-the_cost_of_ad_blocking.pdf
14. GBR research - Consumers fight back in data trust war <http://www.cbronline.com/news/cybersecurity/data/consumers-fight-back-in-data-trust-war-4582508>
15. OECD - Openness and Transparency - Pillars for Democracy, Trust and Progress <http://www.oecd.org/about/secretary-general/opennessandtransparency-pillarsfordemocracytrustandprogress.htm>
16. European Commission - Data protection Eurobarometer http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf
17. Privacy Certification is an important instrument in the upcoming General Data Protection Regulation. Currently there are already certain privacy certification schemes in place, e.g. EuroPriSe, NOREA and ISO 27018.
18. The New General Data Protection Regulation will be enacted early 2016. http://europa.eu/rapid/press-release_STATEMENT-15-5257_en.htm
19. The future of mobile commerce is here. <http://www.weve.com/>



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 Consulting

Postbus 2575 - 3500 GN Utrecht

Tel. +31 30 689 18 50

E-mail: capgeminiconsulting.nl@capgemini.com

www.nl.capgemini-consulting.com