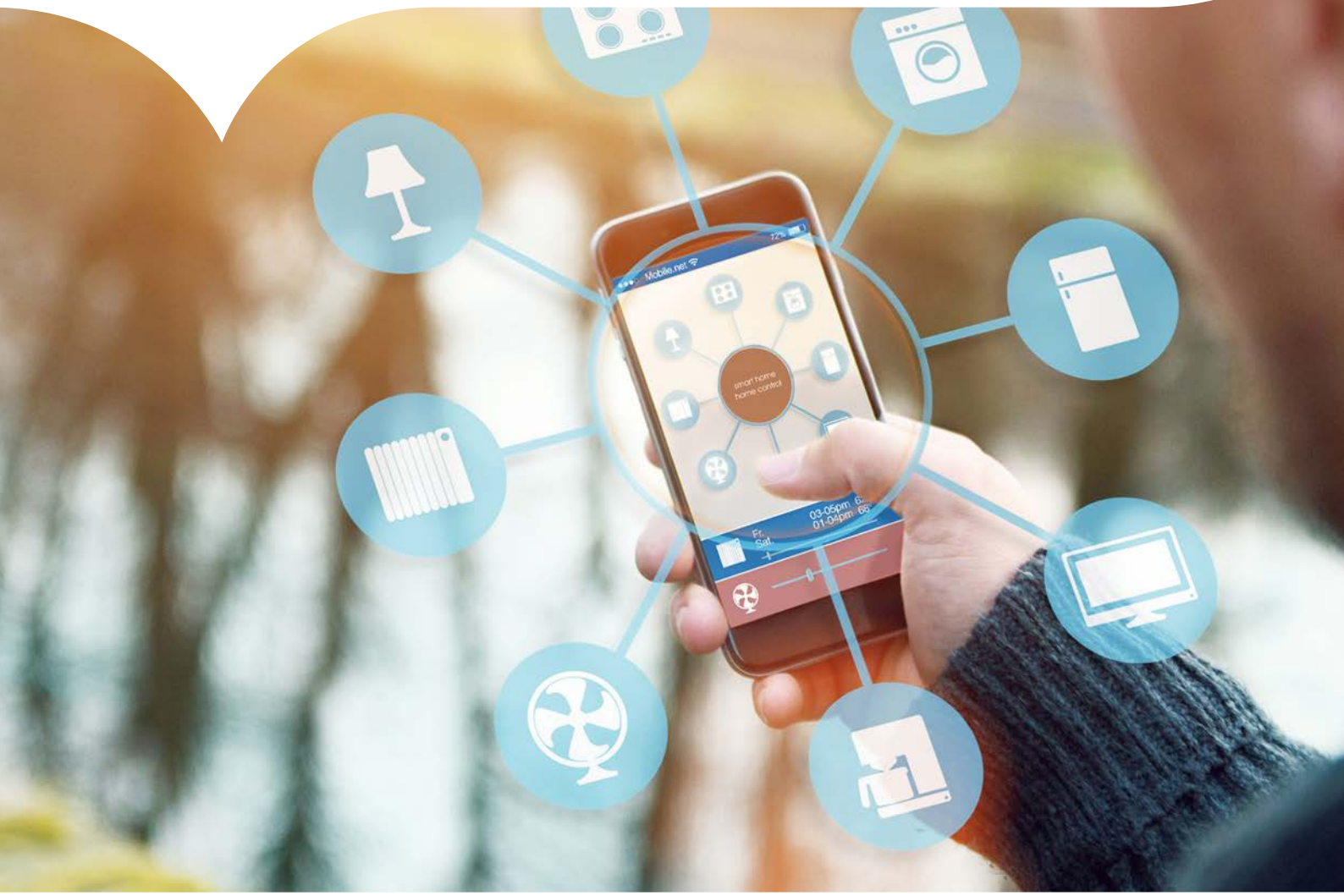
Capgemini Consulting

Privacy in Utilities

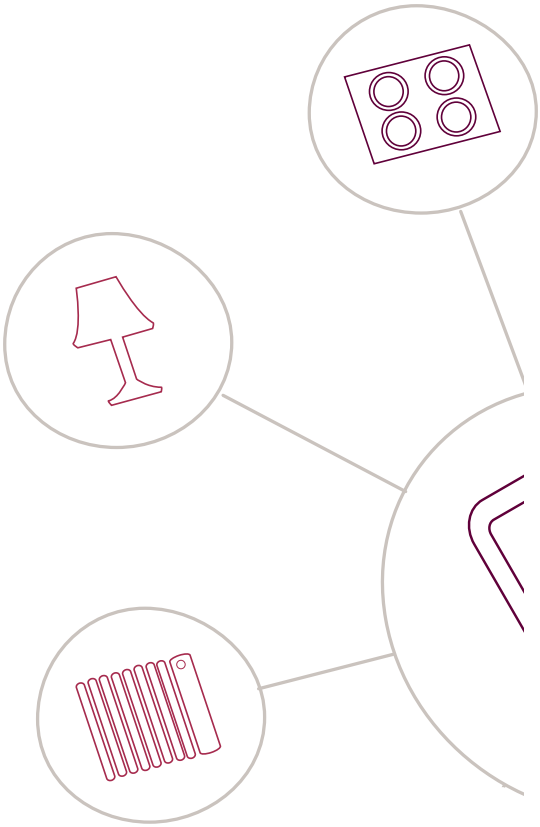
Utilities need to step up their game in privacy to secure the continued trust of their customers



For utility companies, the job of managing their customer's personal data is likely to become much more involved and complicated. And they shouldn't underestimate this task. It is crucial for the continued trust of their customers, and more generally spoken, for their "license to operate". Essentially, there are three distinct reasons:

1. Innovation and the energy transition intensify personal data usage - that comes with a cost

First of all, the future of most utility companies becomes more personal data sensitive as a result of the energy transition and innovation. Smart meters will be deployed across the EU at large scale; that alone accounts for a major increase in the volume of personal data. On top of that, utilities and third party players will



increasingly offer energy related services that require privacy-sensitive data to be shared with them, such as information about when people leave the home or detailed household appliance usage information. And, in response to their slowly eroding traditional business model, many of them will consider to pursue a Smart Home strategy, trying to leverage their current reputation and brand value. This will lead them into spaces where the use of personal data becomes even more significant. As the volume and sensitivity go up, so are the measures to secure the data and maintain compliant with privacy regulation.

2. EU legislation lays the foundation for hefty penalties for non-compliant companies

The General Data Protection Regulation (GDPR) is new regulation and will be enforced by 25 May 2018. Through this Regulation the European Commission intends to strengthen and unify data protection for individuals within the European Union (EU). It allows the European data protection authorities to impose fines of 20M euro, and up to 4% of annual global turnover for non-compliance with its requirements. Since the requirements of this Regulation are strongly business-pervasive and the potential penalties big it is expected that many companies, including utilities, will need to invest significantly in the implementation of GDPR.

These investments fall into two categories: the first category are investments following directly from implementing the Regulation's requirements. Examples are the setting up of a records of processing activities, developing a privacy awareness program for employees, ensuring that a customers' data can be removed entirely from the company's systems or increasing the level of security for certain data sources. The second category are investments into compliancy monitoring itself. Most likely companies will want to move away from dozens of spreadsheets with questionnaires, to more specialized tooling that provide chief compliance officers a much better view on the status of their privacy programs. They simply can't afford to not be in control given the severity of the potential consequences.

3. Data sharing behavior is changing - not in favor of the privacy-ignorant utility

Another reason why we believe senior management will get much more involved in privacy matters, is the fact that it becomes paramount for long-term success of any data-driven company. With growing awareness of consumers for privacy, consumers will increasingly make more explicit evaluations of the trade-off between privacy and added-value of services received. Companies offering services where this is out of balance will see consumers opting-out out or withdrawing their consent to let these companies use their data. On the other hand, privacy well-managed may enable a company to successfully develop new business models, confirm their reputation or reposition itself.

Qiy Foundation

Privacy awareness is increasing - and therefore becoming important

While consumer's privacy awareness is yet far from sufficient, we see it rising. In several European countries Personal Information Management System initiatives are emerging (such as the Dutch Qiy foundation[1] and Mydex CIC (UK)).

Through these platforms consumers can exercise far more control over their personal data and how that is used by companies. Illustrative is also the Dutch "Privacy week" in October 2016. The importance of privacy was addressed through a variety of television formats such as a quiz and a university college-like documentary

[1] https://www.qiyfoundation.org/about-qiy/

where a professor elaborated on how companies use personal data and the implications for individuals. Also a real-life game ("Hunted") was launched where a number of couples try to get out of the hands of a team of hunters that use every piece of intelligence on the fleeing subjects they can get their hands on. It eerily highlights how easy it is for governments to track an individual's whereabouts based on everyday consumer behavior such as withdrawing cash, making purchases, travelling, etc.

These developments signify that it will become important for businesses to incorporate privacy integrally in their product and service strategy. And most companies are not there yet: a survey done by CBR[2] reported 81% of people between 18-24 years admit to provide wrong information when asked for personal information. One of the main causes for this deception is that only 10% believe they will benefit from handing over personal information and 73% are concerned that that they will receive unsolicited contact from businesses as a result.

It's all about trust

Essentially, the key result of privacy being well-managed is having established the continued trust of your customers (and other stakeholders) that personal data is used and protected in a responsible way. Consumers need to trust a company before they are willing to share their personal data[3], and this is crucial to improve customer experience or introduce new data-driven services. The key question is off course: how to gain and keep the trust of consumers over time?

$$\textbf{Trust} = \frac{\text{Intimacy} + \text{Credibility}}{\text{Risk}}$$

Capgemini believes trust can be fostered by realizing three distinct management objectives:

- increasing customer intimacy,
- becoming privacy-credible and
- adopt a risk-based privacy management approach.

Customer intimacy

Companies with higher levels of customer intimacy will find that customers place more trust in them. Intimacy is stimulated by engaging in dialogue and being open and transparent about what you do with personal data. It appears that many companies are lagging in this respect: in March 2015, only 20% of respondents to the European Commission's data protection barometer said they were always informed about data collection and how it was used[4]. And only a fifth said they read privacy statements. It is therefore important to launch a number of one- and two-way communication activities:

- Ask consumers and other stakeholders about their expectations regarding your company collecting data.
- Be open and honest about the purpose of processing personal data. Communicate your privacy commitments clearly to all stakeholders and live up to it.
- Inform consumers about how your company processes personal data in a clear and understandable way. Don't just post a lengthy privacy statement on your corporate website, but critically think through how you can effectively reach your audience and get your key messages across.

[2] http://www.cbronline.com/news/cybersecurity/data/consumers-fight-back-in-data-trust-war-4582508

[3] 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

[4] http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf

Privacy credibility

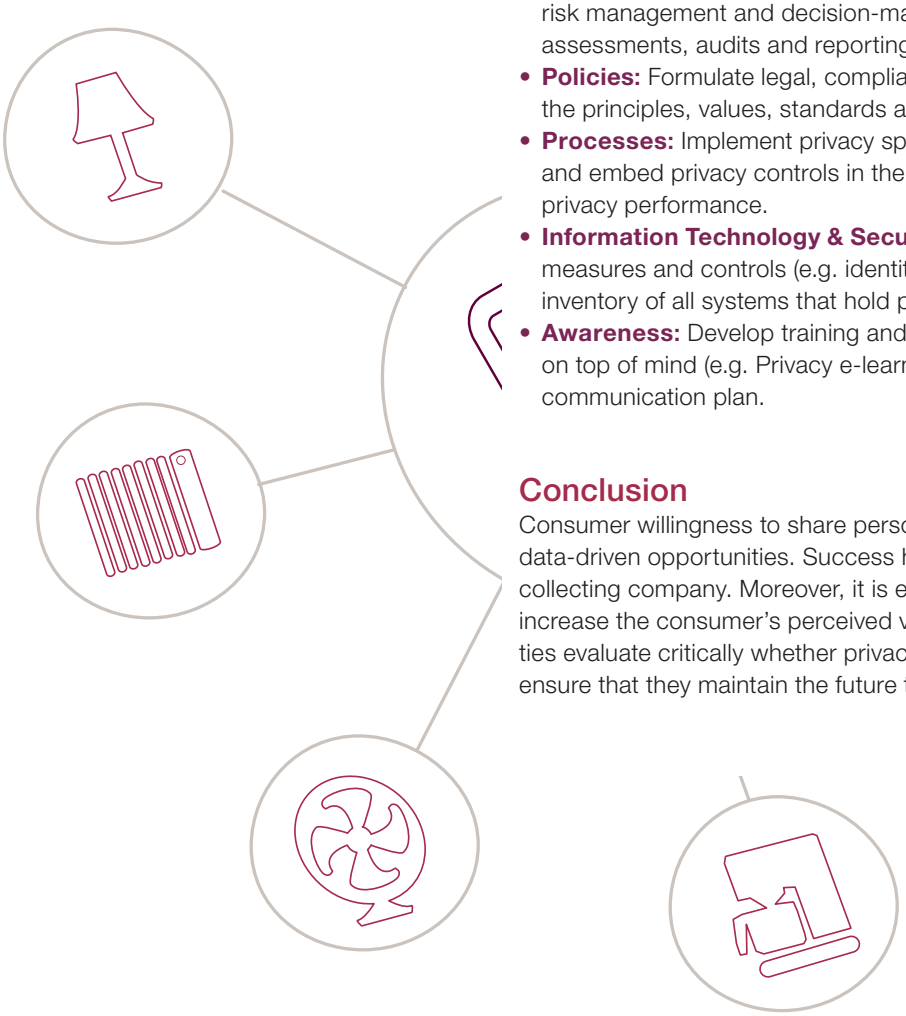
Your company's credibility is strengthened by demonstrating your privacy expertise, your ability to give consumers a voice in the data sharing process and the quality of the consumer data you hold. A selection of credibility-enhancing practices that can be considered in this respect are:

- Develop and demonstrate your privacy proficiency. Consumers expect you to be on top of the privacy regulations and public expectations, for example through privacy certifications. Do good and talk about it.
- 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.
- Genuine consumer consent is a very powerful legitimacy of processing personal data. Support your consumers to understand their data sharing benefits, so they can make informed and conscious choices of sharing their data.
- Provide a single point of truth of the consumers' personal data settings and transactions. Provide insight in consumer profiling, permissions that have been given and with whom their data has been shared.

Risk reduction and compliance

As much as it is important to inform your (potential) customers that you take their privacy seriously, it is to ensure your organization understands the importance ánd enabling them to act accordingly. This is achieved by implementing a mature and effective privacy compliance framework. Pay attention to elements like:

- **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. 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 bring the privacy topic on top of mind (e.g. Privacy e-learning). Support in internal and external privacy communication plan.



Conclusion

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 increase the consumer's perceived value. Therefore it is crucial that individual utilities evaluate critically whether privacy is sufficiently managed in their company to ensure that they maintain the future trust of their customers.

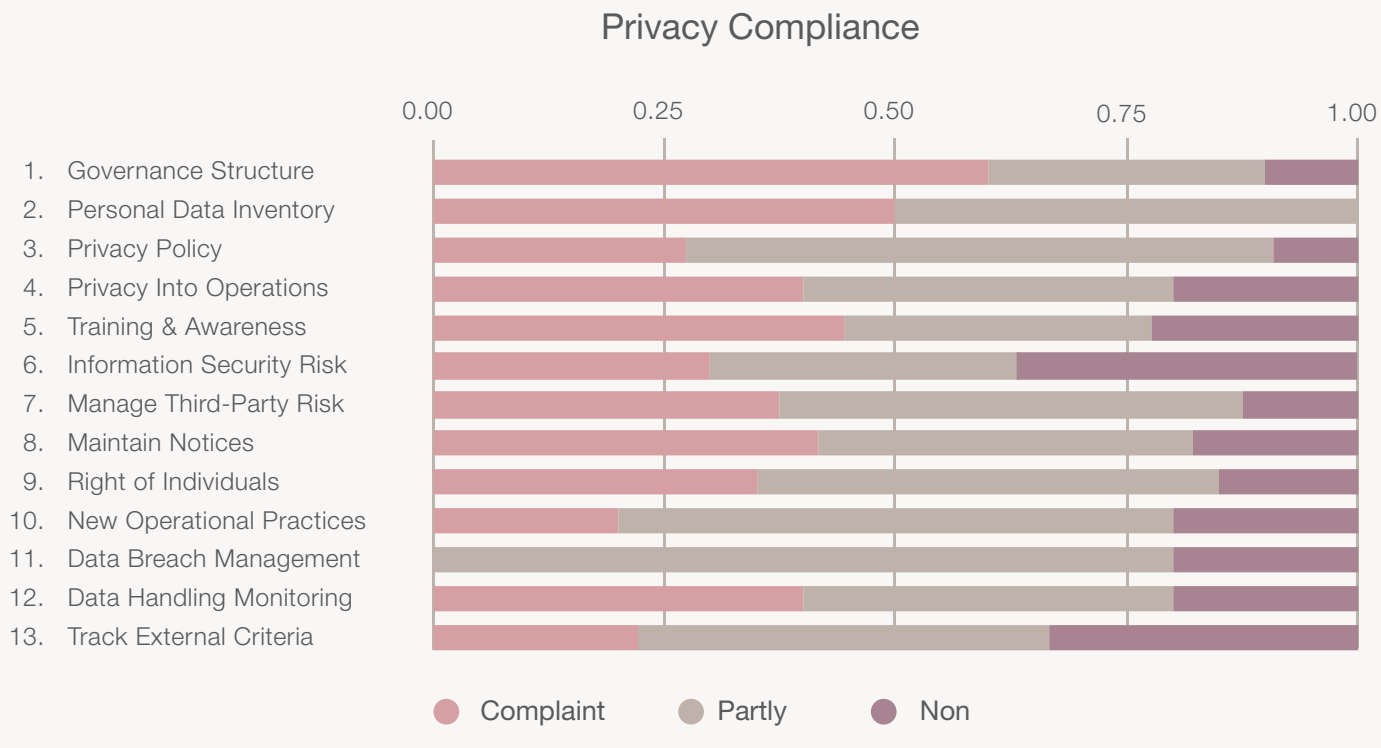
We offer three types of services providing insight and mobilization of stakeholders at different levels in the organization:

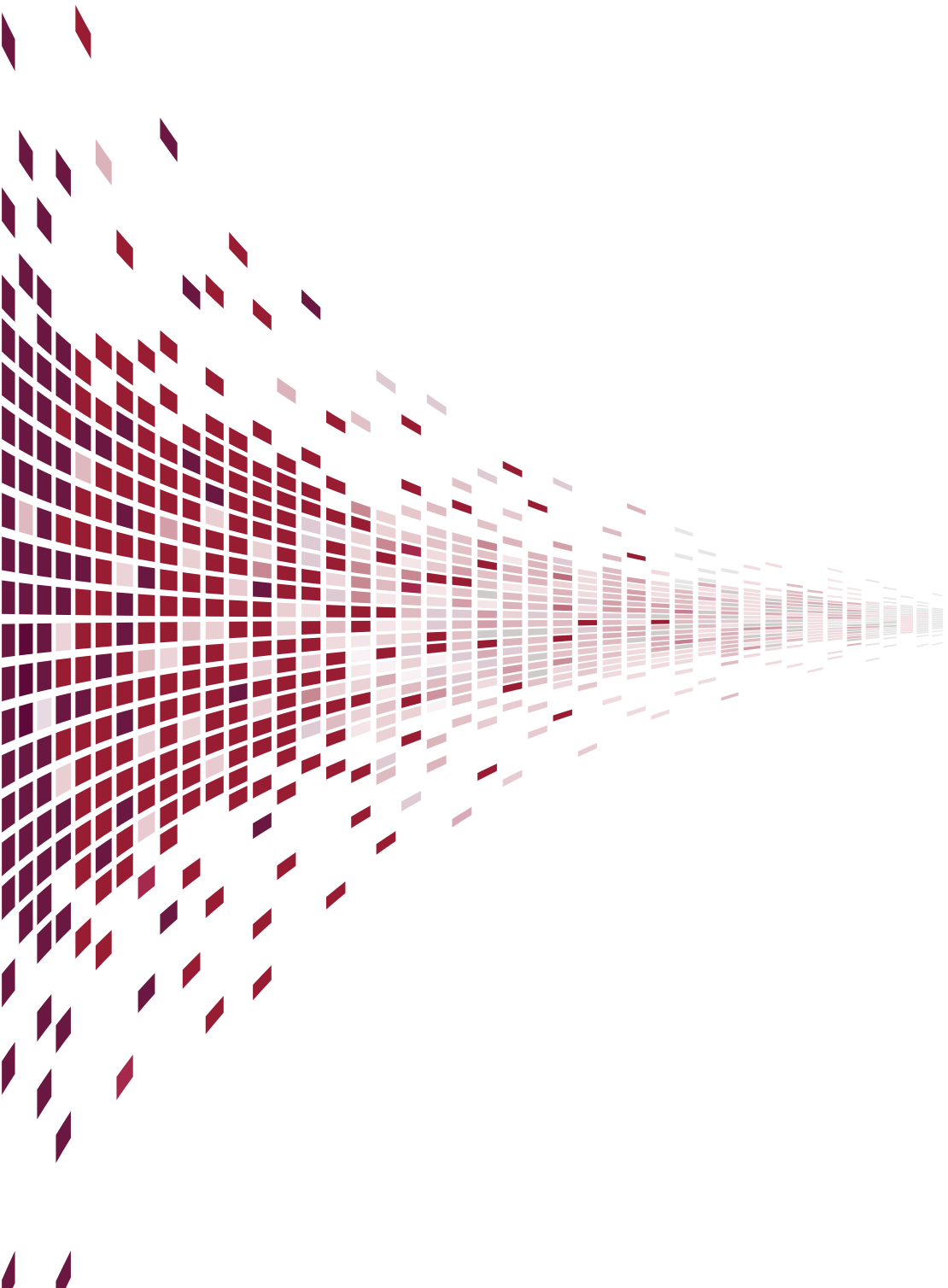
1. **Strategic Privacy Ambition:** the key objective of setting ambitions is to provide high-level insight in the impact of privacy and data protection on business strategy and identify potential strategy execution blockers. It serves to mobilize senior management and set directions for strategic adjustments and/or start a data protection and privacy program. Typically this service is delivered through an executive-level workshop.

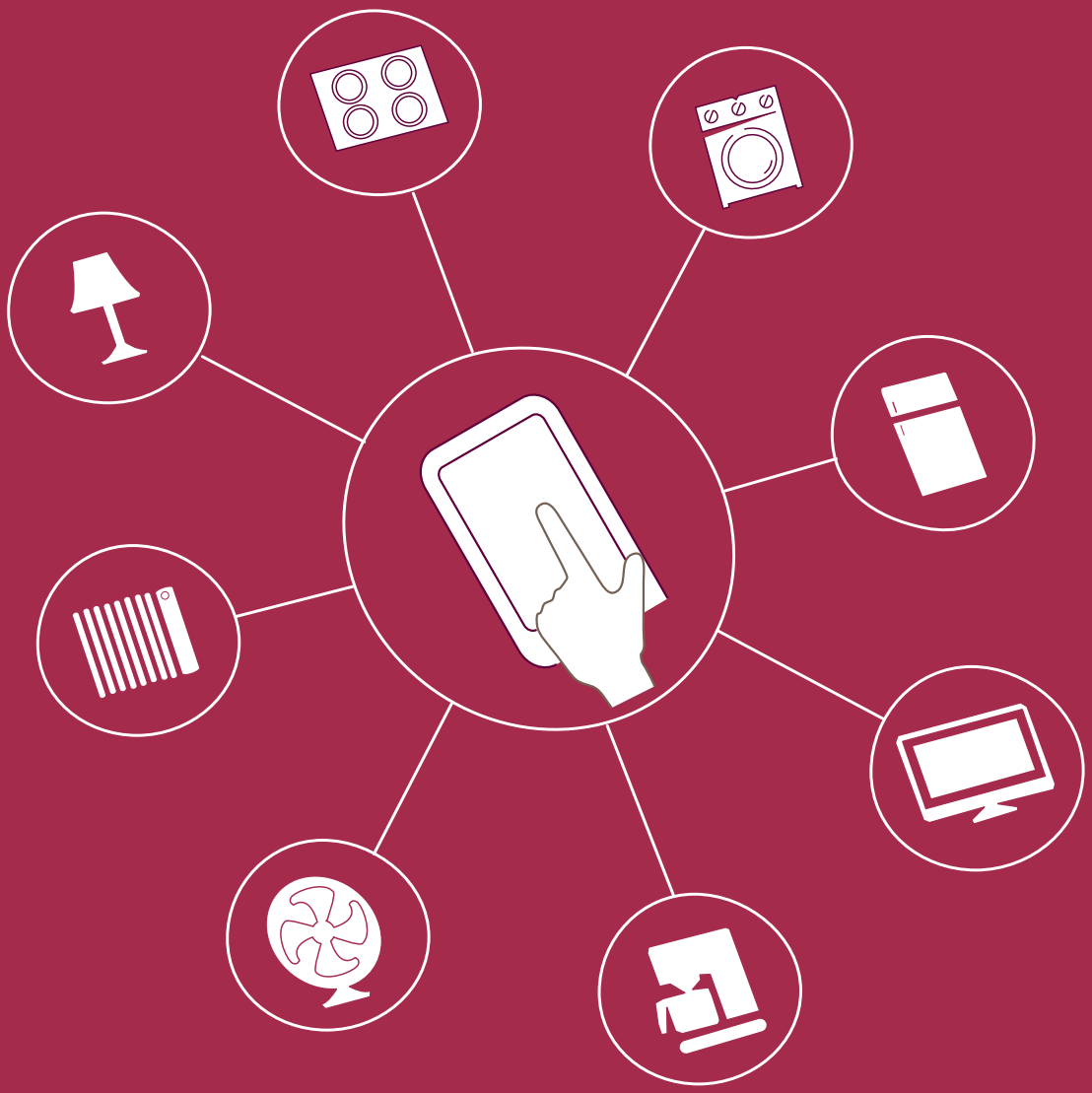
2. **Organizational PIA:** the objective of the Organizational PIA is to determine the needed measures to make the organization privacy-compliant from a governance and policy perspective through application of a standardized framework (NYMITY). It provides insight in the level of organizational compliancy against GDPR baseline and industry peers and delivers a roadmap to close the gaps.

3. **Operations PIA:** the main objective of the Operations PIA is to measure the gap between the privacy policy framework and actual operations (read: processes, systems and the hearts and minds of people). Privacy policies may require an assessment of all of a companies' applications and processes in use, affecting a large number of people in the organisation. We make use of smart tooling to execute and monitor the status of this process, leading to lower project costs and higher effectiveness. A risk-based methodology underlies the approach to ensure assessment effort is prioritized in the right way. We can also lead and/ support the design and implementation of a privacy/data-protection program following the assessment.

Example NIMITY-based privacy compliance report-out







For more information about the challenges of privacy management for utilities or Capgemini's privacy-related services, please contact:

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

Robert Breugem
Analytics & Utilities Consultant
Capgemini Consulting
Email: robert.breugem@capgemini.com
Tel: +31 6 52071 1302

Capgemini Consulting

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 3,000 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.nl.capgemini-consulting.com

Capgemini Consulting
P.O. Box 2575, 3500 GN Utrecht
Tel. + 31 30 689 00 00