ISSUE 20 / JUNE 2019

PECB Insights



DATA PRIVACY OR FREE INFORMATION?

THE 21ST CENTURY DILEMMA

LEADERSHIP STANDARDS EXPERTISE TECHNOLOGY BUSINESS & LEISURE TRAVEL



Catch up with the previous PECB Insights Magazine Issue

- What changes will the revision of ISO 22301 bring?
- How can ISO 45001 help reduce workplace hazards and protect the health and safety of people?
- Is the future of interactive projections just around the corner?
- Can culture transformation be the solution to company development?
- Discover the heart of Europe and experience the upbeat metropole of Prague.

...and more

Read Now! ▶

Inside This Issue

6 Technology

GDPR: Increasing the Privacy Pressure

12 Leadership

The Changing Landscape of Employee Loyalty

18 The Expert

The Wait is Finally Over!

22 The Standard

It's All in the Name: The World's First International Standard for Brand Evaluation just Published

24 The Expert

ISO/IEC 27552: The Answer to Data Privacy?

30 Business & Leisure

Brussels: Europe's Heart Has it All

38 The Expert

An Analysis of the Upcoming NIST Privacy Framework

44 Travel

Coastal California: Two Days in Carmel







The views and opinions expressed in the PECB Insights Magazine do not necessarily reflect the views of PECB Group.

Copyright © PECB 2019. All Rights Reserved


E
S



" IF WE DON'T ACT NOW TO SAFEGUARD OUR PRIVACY, WE COULD ALL BECOME VICTIMS OF IDENTITY THEFT "

Bill Nelson,
Former United States Senator



GDPR: Increasing the Privacy Pressure

The 1-year anniversary of the GDPR has not really flooded the media the same way as it did at the launch.

And I'm not sure what I should think about it today. Mixed feelings, mixed results, because the GDPR sets a consolidated baseline for privacy protection on the EU level but also worldwide, while lots of companies are still in bad shape for their privacy practice, and some old, unacceptable habits are still alive, or even getting worse. So where are we exactly with the GDPR, mid-2019, you think?

1-year baby, growing teenager or grumpy toothless?

First of all, allow me to take a step back: The GDPR is not 'new' - check the GDPR History published by the EDPS. The GDPR applies since May 2018; has been ratified since 2016 has gained political consensus since December 2015; the European Parliament adopted it in 2014, and the data protection proposal was presented in 2012. And actually the GDPR has replaced the European Data Protection Directive 95/46/EC, 23 years later, after its approval in 1995.

An important achievement of the GDPR is that it has (finally) set out the boundaries on a large scale, with a global impact. It has also triggered other nations to align with the new regulations, and that's good news. In contrast to a lot of other legislations, the GDPR is fairly intelligible and readable, so you could guess it would be implemented fairly smoothly.



Still not mature?

Of course, privacy has always been balanced against commercial profit or public 'profit', when talking about governments. For a long time, the weight was rather on the side of commercial profit and performance.

But what is way more important, and where the GDPR is way more distinct than before, is the drive to a practical, reasonable balance between usability and security. You can never secure your data 100%, but you can do your best ('state of the art'). When looking at the GDPR history, you would expect that organizations (including governments) had enough time to get GDPR-ready before the 25th of May last year.

Instead, lots of them got barely compliant and a significant part of them didn't even make it to be compliant. You remember the countdown stress and drama stories, right?

Reality one year later

In practice, many companies didn't see the GDPR coming, or didn't want to see it. They only started to think about the GDPR due to the massive airplay and marketing when the regulation came into force.

But even a basic implementation of a security and privacy management system (like the ISO/IEC 27001 or ISO/IEC 29100 style of management) takes at least a year, even for SMEs.

So they have cut corners because of the predicted GDPR fines, the consent-driven marketing and commercial quick wins ("implement this tech and you're compliant"), and totally forgot about the in-depth quality approach.

There was no time left for privacy-by-design or rather security-by-design, with focus on the subject.

Now, one year later they realize that GDPR compliance is not only about the assignment of a DPO, establishing a processing register, publishing a privacy notice, handling consent and so on. Some companies got bad luck. Now, they know all about handling data breaches, incident management and responsibility vs, accountability of the management team.

Sadly enough, there are still a lot of companies that stay below radar. They don't care and still practice old habits like scraping search results from search engines, dumping personal data from public sources to use for bulk mail and marketing, neglecting subject access requests or minimizing SAR responses like 'we don't process your data'. You can ponder about the reasoning behind it, but it essentially comes down to the idea of getting away with it. Taking into account that the privacy legislation has been there for more than a decade and also the feedback of various data protection authorities have provided (that they would not be too strict on enforcing the GDPR), that's a fail.

Proactive control

From the GDPR side, it would be great to have a more proactive control from EU or data protection authorities and to put more pressure on the compliance of the data controllers. This is sanctioned in the GDPR, e.g. with articles 42 and 43 on certification. But the EU did not provide a ready-to-use system to prove that a company has the minimum precautions and management systems in place to comply with the GDPR requirements. As we see with other legislations and best practices, getting a certification takes time. Now the certification and accreditation battle has only begun, and almost nothing is ready yet. And before you know it, the certification and accreditation will be guided by commercial interest.

I sincerely hope that the EU will guide us with an open system, based on best practices and standards. The EDPB (European Data Protection Board, a.k.a. WP29) already set the guidelines [check the Guidelines 1/2018 (May 2018) on certification and 4/2018 on accreditation (Dec 2018)]. Get ready!





Privacy/security by design

If you wonder what best practices and guidelines could get you on track, you really should look into the established best practices, for example:

- ISO/IEC 27001 & ISO/IEC 27002 for managing your Information Security Management System
- ISO/IEC 27005 for Risk Management
- ISO/IEC 29100 series (privacy framework, publicly available)
- ISO/IEC 29134 for (D)PIA
- ISO/IEC 27035 for incident management (or NIST Incident response).

Further, there are two ISO standards under development for the support of Privacy Information Management (ISO/IEC 27552), and privacy engineering (ISO/IEC 27550).

Referencing to the frameworks and standards, one of the implementation blockers is the lack of free access to the relevant ISO standards (mentioned before). On the other hand, the NIST is providing free access to its framework, but it's US-based and not in sync with GDPR, while the NIST privacy framework is anticipated to be published in October 2019.

The future, new threats & new technology

You don't need to look hard. Even on the regular news (outside the privacy expert channels), you're confronted with decisions, news and activity that puts privacy protection (seriously) under pressure. In many cases, physical threats and cybercrime are the drivers to a very broad 'public protection' or mass surveillance. And in many cases it's the government taking the lead, while there is very low resistance and reasoning to keep it within an acceptable scale. Camera surveillance, ANPR systems, facial recognition, biometric registration, social media surveillance. In the majority of cases, the impact of a crime is significantly inflated to argue the benefits of mass surveillance and to minimize the impact on the general audience.

This approach makes it extremely hard to have a balanced discussion and choose the right level of protection. Just a look at a few recent news items, just to name a few that passed by on my privacy feeds:

"If you've got nothing to hide, you've got nothing to fear: fingerprints on Belgian eID cards."

(BELGIUM, 15 JANUARY 2019, KU LEUVEN)

Facial recognition system in the UK: legal case against police

(BBC, 21 MAY 2019)

Civilian protest against cameras

(DAILY MAIL, 16 MAY 2019)

Just as an example, as of the 1st of July, the Belgian police will not use the ANPR system only 'against terrorists', but will use it to detect traffic offense. So, we are well on our way for Big Brother 1984. Moreover, how do you balance privacy against a visa application demanding for all of the social media profiles plus the 5-year-history of your mail and phone contacts? (Source: BBC, 1 June 2019). Don't say it could not happen to you in the EU. It only requires a new election of the president, prime minister or change of government to start a short term political change.

You need to set the bar on your privacy

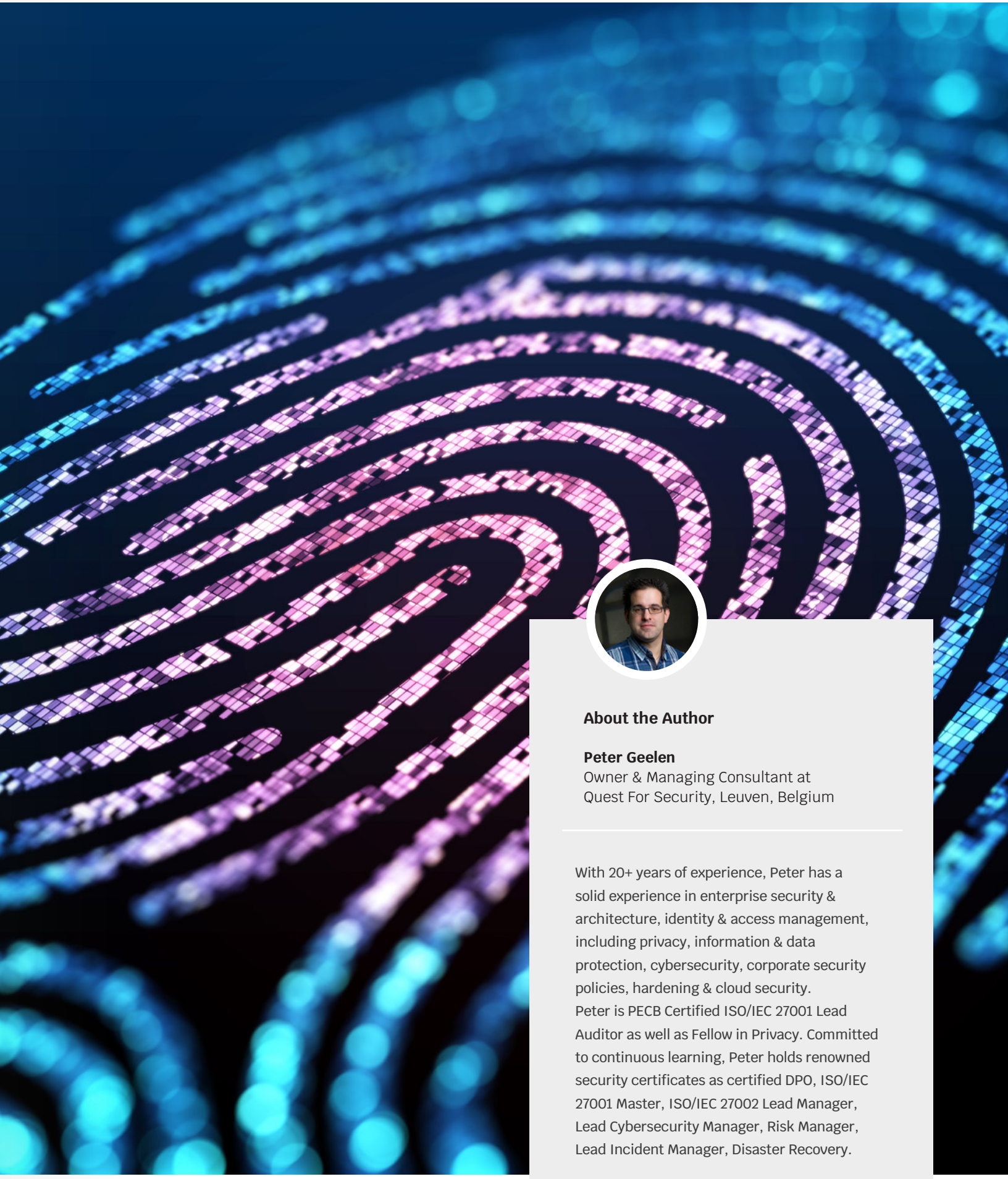
The GDPR has provided the baseline to get the data protection you deserve. But the bottom line is: you'll only get the privacy when you demand it. ("Fight for you right.") And more importantly, companies, governments, any data controller, any person will only respect your privacy if it really can hurt them. You must be part of their risk management. Some EU countries already incorporated the GDPR in their national legislation a while ago. Leading by example, they brought some companies to court. On a European level, wider scale enforcement of the GDPR is slowly warming up. The Belgian DPA only applied their first fine a few weeks ago to a mayor using emails for the past EU elections.

So where to go from here?

As a company, instill the GDPR in your DNA – in everything you do. It's never too late to do it right. As a person, you can enforce the adoption of data protection step by step. Don't wait for someone else to speak out for you. The best advice I've taken, was 2 months ago from a television broadcast on the abuse of personal data – *(Translated quote)*:

"Every time you give away a piece of your personal data, just think it's € 50 you give away."

That is a great tip to let go your timidity and be more assertive. Be careful what you share, and use the rights that the GDPR grants you to stay in control. Actively. And if you don't know what the GDPR can do for you, dive into it. It's never too late.



About the Author

Peter Geelen
Owner & Managing Consultant at
Quest For Security, Leuven, Belgium

With 20+ years of experience, Peter has a solid experience in enterprise security & architecture, identity & access management, including privacy, information & data protection, cybersecurity, corporate security policies, hardening & cloud security.
Peter is PECB Certified ISO/IEC 27001 Lead Auditor as well as Fellow in Privacy. Committed to continuous learning, Peter holds renowned security certificates as certified DPO, ISO/IEC 27001 Master, ISO/IEC 27002 Lead Manager, Lead Cybersecurity Manager, Risk Manager, Lead Incident Manager, Disaster Recovery.

The Changing Landscape of Employee Loyalty

"You just can't expect loyalty from employees anymore," is a common lament heard across many industries today and in my view, it's entirely correct. However, the cause of reduced employee loyalty is not so much about the employees as it is about employers failing to recognize the needs and expectations of employees in a competitive global marketplace today. Loyalty can no longer be expected, rather, it must be earned.



LinkedIn did some interesting research with their Talent Trends 2014 survey which found that only 15% of employees are so satisfied with their roles that they are not open to looking at new employment opportunities. Fifteen years working as a business coach has taught me that any organization with an employee turnover problem is one that has significant leadership and culture problems. With the cost of replacing employees estimated at around 1.5x their annual salary, it pays to retain great staff. In this article I'm going to outline what you can do through a simple R.E.T.A.I.N. formula to ensure you keep your best employees loyal to you and your business. Considering the Talent Trends data along with the latest Employee Exit Survey, (also by LinkedIn) data shows that two thirds of employee turnover could be prevented by





addressing three common issues causing employees to change jobs: a lack of advancement opportunities (22%), unsatisfactory leadership or senior management (19.5%) and experiencing a lack of challenge in their job (13.8%). All three of these reasons point directly back at issues with leadership and management. Let's address each one of these in turn.

Issue #1: A Lack of Advancement Opportunities

Have you ever heard the phrase, "Perception is reality"? What I see in many businesses is managers so busy that they struggle to sit down once a year with their staff to review their performance and career goals. Employees adore managers who are prepared to say, "I believe in you" and help stretch their vision and create brightness of future for their career. Many managers also fail to create a career plan with milestones and goals to keep employees engaged and passionate in their roles. As an employer, you need to encourage and support your employees in improving their skills and education. Prepare and invest in training your people to be ready to perform at the next level well before the job opening comes up. It really helps to have a "hire from within" employee mobility policy that gives preference to your existing employees when applying for new roles that open up within your organization. It's a lot more inspiring for the team to see colleagues being promoted than new people being hired from outside. This policy also protects and reinforces your company culture.

Issue#2: Unsatisfactory Leadership or Senior Management

Someone being a star performer in his/her allocated role does not mean that they are great management material. Technical skills and people skills lie at opposite ends of the behavior spectrum and very few companies invest in grassroots level leadership programs to encourage and grow soft skills and leadership at all levels. Leadership programs tend to be reserved for senior managers, however, by then, it is often too late.

Practicing any new skill without appropriate training creates bad habits and poor outcomes. Imagine giving your teenage children the keys to the car and telling them, “Give it a go, you’ll figure it out.” There’s a significant chance they will end up injuring themselves and any other unfortunate soul who gets in their way. The same is true for any employee or manager in your company that is promoted without adequate training. The casualties end up being your staff and your customers. Practice makes perfect only when the practice is performed correctly.

It is critical to regularly set aside time to engage with and listen to your employees. Ask them to rate your performance as their manager. When employees feel like the management is listening, they feel valued and their motivation increases accordingly.

Issue#3: A Lack of Challenge in Their Job

This is again where managers fail to really understand their employees or to challenge them with stretch goals or innovation projects. Any job can be fulfilling if the person understands the importance of what they are doing and receives recognition and appreciation from colleagues and managers for a job well done. Implement data collection programs so you can regularly monitor how your employees are performing on key responsibilities.

Why not come up with some additional projects for your employees to work on in their spare time? Reward entrepreneurial thinking (or intrapreneurship) – your staff often know where the problems and opportunities lie within your business; if they can help you increase revenues or reduce costs, why would you not reward them accordingly? One example of this is the Whole Foods Market that gives their store managers an annual budget to test new ideas. One manager came up with the idea of building a craft beer tap room in their store and it became such a huge success it was rolled out to most of the stores across the network.



We Need to Address Changing Employee Expectations

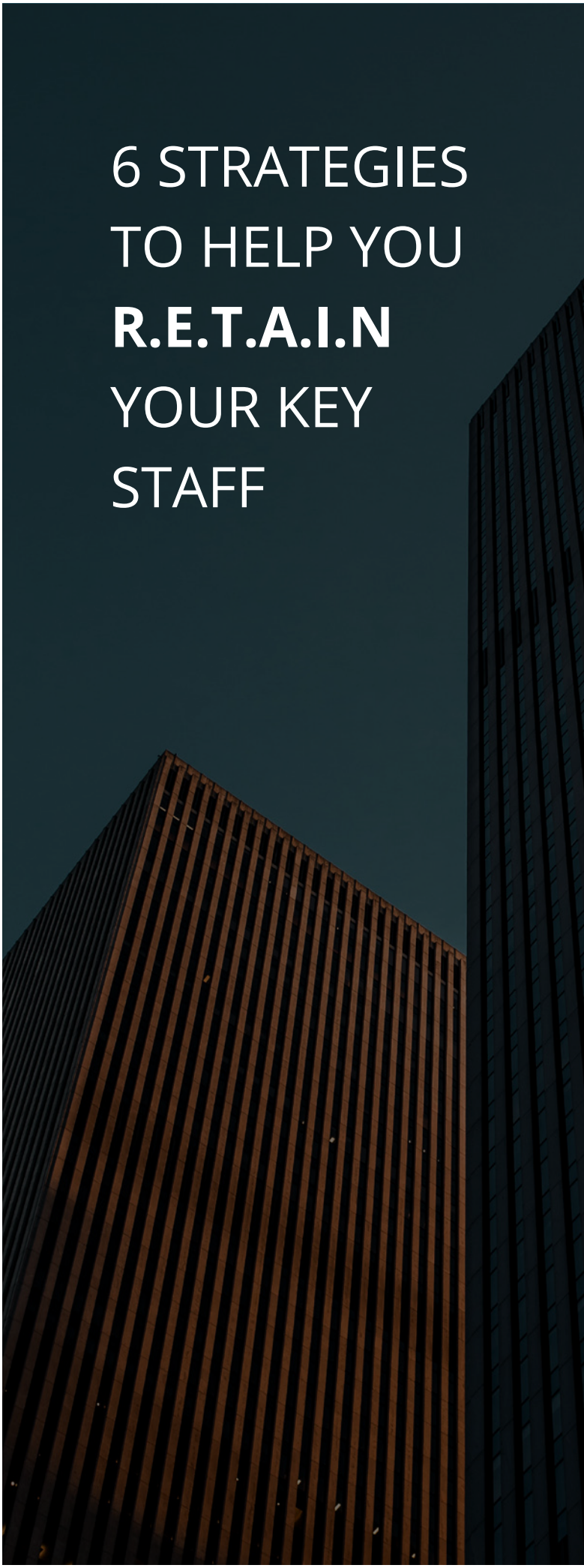
The average employee entering the workforce today will work for more than 7 organizations in their working career. Employees (especially Gen Y and Millennials) want to maximize their chances of remaining employable and obtaining career advancement, so they often look to work for multiple employers to rapidly grow their skill and knowledge base.

One of the unwritten rules of leadership (and life) is that you get what you give. The more value you give, the more value will come back in return. So you need to stop looking at your employees with the perspective of what they can give you. Instead, take some time to reflect on what value you can give to them.

Employees don't leave companies; they leave their managers and colleagues. If you create an environment where employees enjoy coming to work, get the ability to use their skills in a meaningful way, and are given the opportunity to learn, grow and master new skills, then they are very unlikely to want to go anywhere else. If they do, they will quickly want to come back when they realize the many things they had been taking for granted working for your organization.

So what does this mean in the context of increasing employee loyalty?

Leadership, pure and simple. As a leader you need to be able to articulate the vision of where your organization is headed and the role that the team members need to play in making it a reality. You need to know your employees as individuals and to communicate the potential that you see within them and the career opportunities your organization will provide them if they deliver on what is asked of them. Create a bright and compelling future that your team is excited about and they become self-motivated.



Relationships
Understand that building and protecting relationships must come first. Teams that play together, stay together. Build relationships with your employees both inside and outside the workplace.

Education
Have a career development plan and training budget for each of your employees. Even if promotion is unlikely, it is important that people are given the opportunity to learn and grow within their roles.

Talk
Speak with your staff in groups and one on one regularly. Let them know how they are doing. Be sure to listen and take on-board employee feedback, especially before making decisions that affect them.

Accountability
When you promise to do something, do it. Likewise, ensure you follow up and hold all team members accountable also. This is one of the most important keys to building a high-performance team as it builds trust.

Inspire
When you make your staff feel like they are part of an important cause and that their work is important and valued, it adds to their job satisfaction and motivation.

Notice
Catch your staff doing things right and give them recognition and appreciation for a job well done. What gets measured, gets done; what gets rewarded, gets repeated.

You may notice that all of the six strategies outlined are related to communication. Great communication is delivered face to face, not via email. Technology has increased productivity but has failed to create the paperless office or to reduce employee workload. Employees now expect and demand more flexible work arrangements and it's critical that you as a manager communicate effectively to understand their needs and balance this with your organization's needs to create a long-lasting and mutually beneficial relationship for all parties.



About the Author

Jeremy Carter
CEO – Chief Enthusiasm Officer
Rapport Leadership International

Jeremy has worked as an executive, business and leadership coach, speaker and trainer for the last fifteen years. His passion is helping people to become better leaders and to experience greater levels of success in their lives. He works with organizations across Oceania and Asia to build high-performance cultures to attract and bring the best out of their team members. Jeremy believes strongly in community service and is the President of his local Rotary club as well as mentor local charities. He regularly speaks at conferences on leadership and high-performance teams and delivers public and in-house training courses mentoring future managers and leaders. A thought leader, Jeremy has been featured in the Sydney Morning Herald, Australian Financial Review and Daily Telegraph as well as magazines including CIO, APAC CIO Outlook and Face2Face. His leadership articles on LinkedIn have resulted in him attracting an audience of over 15,000 followers.



The Wait is Finally Over!

KPMG Canada has partnered with PECB to provide Privacy by Design Certifications putting those businesses that embed privacy into their mode of operation at a competitive advantage.

Privacy by Design was first a concept, then law under the General Data Protection Regulation (GDPR), and is now an under-development-ISO standard (PC/317 - ISO 31700). The Privacy by Design Certification finally allows organizations to operationalize Privacy by Design with the objective of ensuring that privacy is embedded into new technologies and business practices.

Privacy by Design: A Risk-Management Solution

In recent years, digital privacy and security have been at the forefront for many organizations which collect personal data. Strict privacy regulations have recently come into force as a result of the prevalent misuse of personal data and rise in breaches.

Consumer trust is at an all-time low. To succeed in the digital economy, companies not only need to comply with regulations, but they also need to instill ethical data practices to earn the trust of their consumers, which in turn will enable them to succeed in a competitive environment. There is no better way to show an organization's commitment to privacy and dedication to trust than through a Privacy by Design Certification.

Privacy by Design builds on the premise that privacy should be embedded into the design, operation, and management of IT systems, networks, and business practices in order to prevent privacy vulnerabilities and the potential for irreparable financial and reputational harm.

Originally developed by Dr. Ann Cavoukian, former Information and Privacy Commissioner of Ontario, Privacy by Design is now law under the EU's GDPR and globally recognized as an ISO standard being developed by ISO/PC 317 Committee for Consumer Protection: Privacy by Design Consumer Goods and Services.

Privacy by Design is structured around 7 Foundational Principles, which exist as a baseline for robust data protection.

1) Proactive not Reactive – Preventative not Remedial: Privacy by Design anticipates risks and prevents privacy-invasive events before they happen.

2) Privacy as the Default Setting: Personal data should be automatically protected – no action is needed by the user to protect their privacy – it is built into the system.

3) Privacy Embedded into Design: Privacy is embedded into the design and architecture of IT systems, and becomes part of the product, service or processes' core functionality.

4) Full Functionality - Positive Sum, Not Zero Sum: Privacy by Design avoids the false idea of trade-offs between privacy and security, showcasing that it is possible to have both.

5) End-to-End Security - Lifecycle Protection: Privacy by Design embeds security into the system from the start, ensuring cradle-to-grave secure lifecycle management of information.

6) Visibility and Transparency - Keep it Open: Privacy by Design ensures that operational execution aligns with policies. The end user should know which data is collected, and for what purpose.

7) Respect for User Privacy - Keep it User-Centric: Privacy by Design develops trust by choosing user-centric measures - strong privacy defaults, appropriate notice, and empowering user-friendly options.

A Privacy by Design Certification demonstrates an organization's proactive, risk-based approach to building a true due-diligence defense in the event of a privacy breach, investigation and/or complaint.

Two-Step Process to Achieving Best-In-Class Privacy Standard

KPMG has partnered with PECB to launch the Privacy by Design Certification Program in which KPMG will serve as the exclusive assessment arm for Privacy by Design Certification by PECB.



Obtaining a Privacy by Design Certification is a two-step process:

1.Assessment: Taking a holistic, risk-based approach, KPMG assesses an organization's product, service, process or system using an assessment framework structured around the 7 Foundational Principles of Privacy by Design, international privacy legal requirements (e.g. GDPR), privacy and security standards, and industry best practices.

The assessment framework also incorporates considerations for emerging technologies such as AI, IoT, mobile devices, and blockchain. The assessment is conducted through a set of interviews with key stakeholders and a review of documentation.

An organization's current privacy controls and information handling practices are reviewed to assess whether the organization meets the applicable criteria. Once the assessment is complete, KPMG will issue a report with areas that need improvement or are not compliant with the framework. The organization will have the opportunity to remediate those identified gaps.

Once implemented, KPMG will conduct a focused reassessment to ensure the initially identified gaps meet the controls. Once KPMG is satisfied that the organization meets the criteria in the assessment framework, the organization will be issued a Privacy by Design Assessment Report with a positive or negative recommendation for certification. Then, the assessment report will need to be sent to PECB for review.



2.Certification: PECB reviews the assessment report and if satisfied on its criteria set forth in the PECB Privacy Certified standard and Privacy by Design framework, it will issue a Privacy Certified Certificate for Privacy by Design for the organization's process. The certification can be displayed on the company product offering for three years, subject to renewal.

Implement the Solution; Obtain the Results

Obtaining a Privacy by Design Certification, as a risk-based solution, leads to positive results. Privacy by Design Certification serves as a valuable tool to achieve a "defensible position" and demonstrate a proactive risk-based approach to minimize risk. It also serves as a competitive advantage to earning consumer trust and loyalty with new technologies, services, or processes.

About the Authors



Sharon Bauer, BA LLB
Senior Manager, Privacy, Regulatory & Information Management
KPMG Canada

Sharon is a Senior Manager in the Digital Privacy, Regulatory, and Information Management practice at KPMG Canada. She helps organizations understand their governance structure, organizational & compliance risks, and privacy risk posture. She also builds strategic plans to support large-scale digital transformation projects and helps organizations optimize their business solutions to ensure alignment with regulatory expectations, industry standards and best practices. Sharon leads the Privacy by Design Certification Program at KPMG.



Sylvia Kingsmill, BA LLB
Partner, National Lead, Privacy, Regulatory & Information Management
KPMG Canada

Sylvia has over 15 years of experience providing strategic, risk management and compliance advisory services, serving both the public and private sectors. She advises executive teams on data-driven digital strategies to support major business transformations in alignment with new regulations, policy and data governance trends, having successfully deployed data analytics platforms and national data registries.


AMERICAN EAGLE OUTFITTERS
H&M
MARRIOTT MARQUIS
Disney
BEAUTY AND THE BEAST
NOW IN
"INSPIRATIONAL AND HIGH-SPIRITED."
BEST MUSICAL
GROUNDHOG DAY THE MUSICAL
CATS
16 ORIGINAL CREAMERY FLAVORS
CYNDI LAUPER
TOSHIBA
THE DEFENDER
EXPRESS
McDonald's
AMERICAN EAG

It's All in the Name: The World's First International Standard for Brand Evaluation just Published

A brand can be a company's most valuable asset. Yet how do you know what it's really worth? Measuring the value of a brand starts with knowing what to measure – and how. The world's first International Standard for brand evaluation will help, and it's just been published.

No-one wants to pay 'just for the name' yet branding power means we often do. One of those intangible but valuable things, branding influences the decisions of customers, financial institutions, potential buyers of the business and more. And some brands are worth a lot.

Yet not all measures are monetary and there are many different approaches and methods used around the world, which makes true comparisons and benchmarking somewhat tricky.

ISO 20671, Brand evaluation – Principles and fundamentals, aims to standardize the technical requirements and evaluation methods involved in brand valuation. It complements ISO 10668, Brand valuation – Requirements for monetary brand valuation, which focuses primarily on the financial aspects.

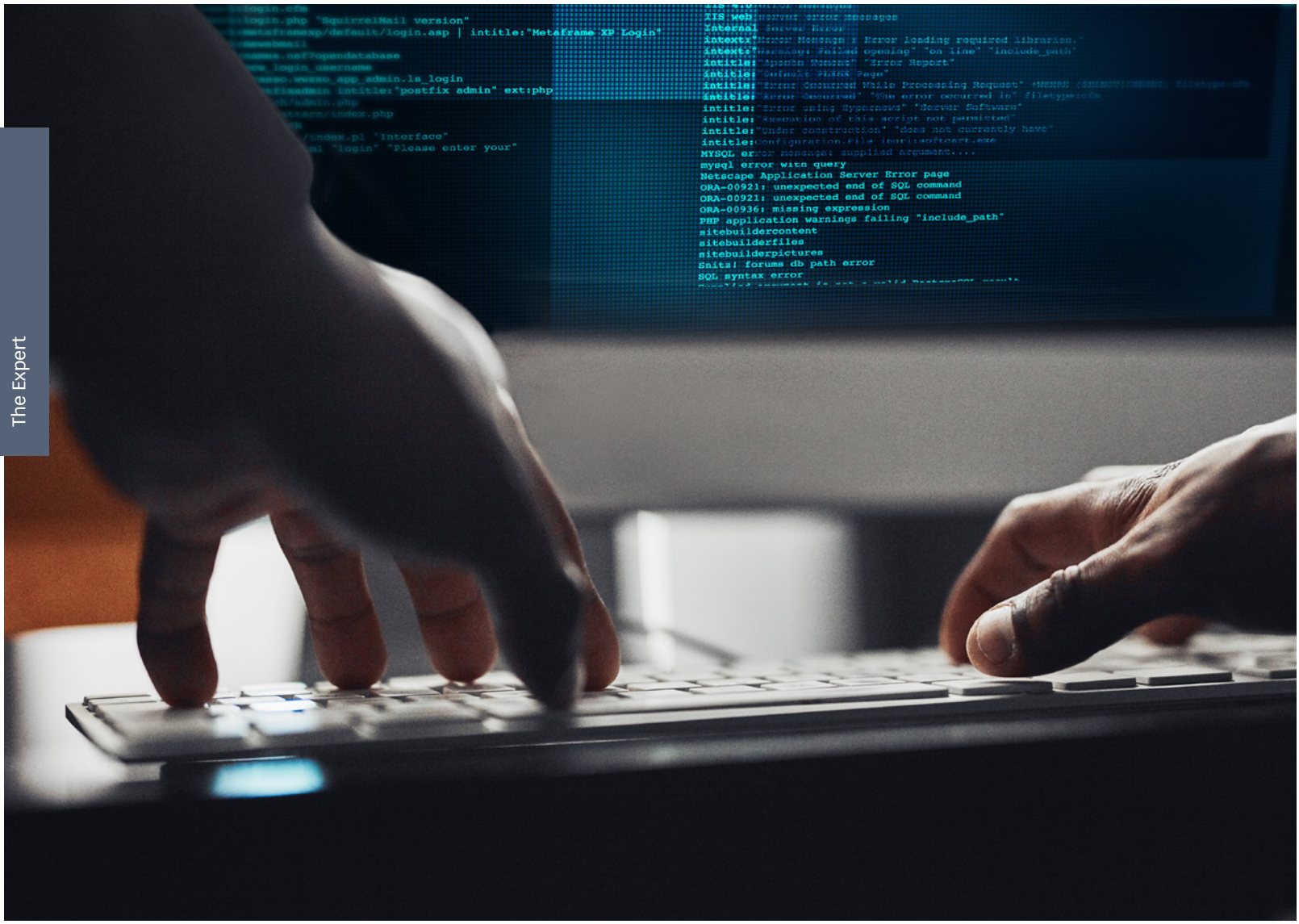
ISO 20671 was inspired by the Austrian standard, ONR 16800 Method for the evaluation of the intangible asset brand, published in 2006. It was the first ever standard on brand evaluation, and was developed by Austrian Standards, ISO's member for Austria.

Dr. Gerhard Hrebicek, who was chair of the committee that developed ONR 16800 and played a role in the development of ISO 20671 said the standard starts a new era for brands.

"ISO 20671 is aimed at businesses of all kinds wishing to increase their brand value and provides a starting point for high-level planning and governance, including best practices for brand management and brand reporting. It provides a more holistic view, covering non-financial as well as financial measures, and forms the basis for other, more specific standards to be developed."

Dr. Bobby Calder, chair of the ISO technical committee that developed ISO 20671 added: "ISO 20671 covers all the factors that influence the success of a brand, such as innovation, tangible resources, service and quality, as well as brand strength and performance. All of which can have an impact on the monetary value, and thus, by measuring them, businesses can more easily identify areas for improvement or investment."

Disclaimer:
*PECB has obtained permission to publish the articles written by **ISO.***



ISO/IEC 27552: The Answer to Data Privacy?

The information security community is excited about the upcoming ISO/IEC 27552 –Privacy Information Management, which is an extension to ISO/IEC 27001 and 27002. Personally, while I am certified in GDPR, I have worked with the new California Consumer Privacy Act, and am familiar with South Africa's' Protection of Personal Information Act (POPIA, Asia Pacific Data Protection and Cyber Security Regulation, as well as many other acts and standards), I still feel that all these standards are lacking in different areas. This new ISO standard provides guidance on the areas that are needed for the implementation of a robust privacy program and fills in the gaps that are missing in so many acts and standards pertaining to Personally Identifiable Information (PII)/ Personal Data.

The GDPR for instance, does require security and does list controls as seen in Article 32: "Security of processing data", but it does not give detailed guidance. ISO/IEC 27001 is a great standard for Information Security Management System (ISMS). Annex A of this standard provides 114 controls for implementation to help protect the organization and the confidentiality, integrity and the availability of data. ISO/IEC 27002 provides the implementation guidance for ISO/IEC 27001 and is a code of practice for information security management. Now, by also implementing the upcoming ISO/IEC 27552, these standards can help you be compliant with many data privacy regimes, requirements and acts.

Much Needed Annexes

Fortunately, Annex C of ISO/IEC 27552 – Information Privacy Management System (IPMS) is a mapping of the ISO/IEC 27552 and articles 5 to 49, except article 43 of the GDPR. The other Annexes are helpful as well:

- Annex A contains PIMS-specific reference control objectives and controls (PII Controllers).
- Annex B covers specific reference control objectives and controls (PII Processors).
- Annex D of ISO/IEC 27552 provides a mapping to ISO/IEC 29100 Information technology -- Security techniques -- Privacy framework. The PECB whitepaper on ISO/IEC 29100 defines its use as “intended to be used by persons and organizations involved in designing, developing, procuring, architecting, testing, maintaining, and operating information and communication technology systems where privacy controls are required for the functioning of PII.”
- Annex E maps ISO/IEC 27552 to both ISO/IEC 27018, which is a code of practice that focuses on protection of personal data in the cloud and ISO/IEC 29151, which establishes control objectives, and guidelines for implementing controls, to meet the requirements identified by a risk and impact assessment related to the protection of Personally Identifiable Information (PII).
- Annex F includes a common terminology and alternative terms to help with documents that have similar or identical meanings as those used in the standard.
- Annex G contains information on how to apply ISO/IEC 27552 to both ISO/IEC 27001 Information Technology Security techniques and ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security controls.

Privacy and Security Management Systems

I utilize ISO/IEC 27001 so often in consulting and audit projects that I feel I have it memorized. I also teach PECB ISO 27001 Lead Implementer and Lead Auditor courses. However, as much as I am a fan of ISO/IEC 27001 and ISO/IEC 27002, they address Information Security implementation and maintenance, and not so much privacy and Personally Identifiable Information. Therefore, other addendums, like the ISO/IEC 27552 are indeed needed to address compliance with Personal Data Requirements.PECB will launch an ISO/IEC 27552 training course soon. In terms of meeting the challenges of maintaining information security and implementing the measures to protect the data, ISO/IEC 27001 is excellent standard, but it does not go into depth in all areas of PII/Personal Data requirements. It is a good management standard providing a general framework that helps to protect information relating to privacy. There are many standards in the 27000 family and ISO 27001 by itself cannot meet the demands that are required for privacy. This is evident by the number of ISO standards that are included within the annexes of ISO/IEC 27552 as outlined above. The IPMS requirements related to ISO/IEC 27001 and ISO/IEC 27002 are well organized in the standard.

- Requirements related to ISO/IEC 27001 are outlined in clause 5.
- Requirements related to ISO/IEC 27002 are outlined in clause 6.



The guidance provided for Controllers and Processors is very useful and detailed:

- PII Controllers guidance is outlined in clause 7.
- PII Processors guidance is outlined in clause 8.

Compliance with Multiple Standards

This standard will be of great help to organizations in developing privacy regimes that will comply with multiple requirements from the GDPR to support European Citizens to the US privacy requirements of the California Privacy Act and the Health Insurance Portability and Accountability Act (HIPAA), as well as others that are forming to put controls in place to give better rights to individuals and to better manage privacy. Through taking the best of each of the existing privacy standards and amalgamating them with ISO/IEC 27552, this standard reduces the burden of managing different privacy standards into a cohesive standard that includes mapping to many other standards. The approach of ISO/IEC 27552 will help organizations establish, implement, maintain, and continuously improve their privacy programs. This will certainly help PII controllers and PII processors. Having a standard that is accepted worldwide will help in doing business internationally, and help protect PII information uniformly around the world. A critical requirement of PII is transparency and communicating compliance to stakeholders. Clients, customers and other stakeholders want to know that an organization they are entrusting with their PII, is doing all it can to be compliant. Companies which will be compliant with ISO/IEC 27552 – Information Privacy Management will stand out as having a strong commitment to meeting and maintaining privacy standards and while providing more certainty to their stakeholders.

Headlines of breaches of data in 2018–2019 were plentiful. Some examples include:

IN THE UNITED STATES:

"ACCORDING TO THE RESEARCH, PERSONALLY IDENTIFIABLE INFORMATION (PII) WAS THE MOST TARGETED DATA FOR BREACHES IN 2018, COMPRISING 97% OF ALL BREACHES."

Per Security Magazine June 4, 2019

IN THE UNITED STATES:

"2018 IN NUMBERS: DATA BREACHES COST $654 BILLION; EXPOSE 2.8 BILLION DATA RECORDS IN THE U.S."

Per Net Security Magazine

IN THE UNITED STATES:

"2.8 BILLION US CONSUMER RECORDS LOST IN 2018; HEALTHCARE BREACHES GREW 400%, STUDY SHOWS"

Per Dark reading June 4, 2019

IN THE UNITED STATES:

"QUEST DIAGNOSTICS DATA BREACH PROMPTS AGS PROBE IN 2 STATES, CLASS ACTION IN ANOTHER"

Per Connecticut Law Tribune June 7, 2019

IN SOUTH AFRICA:

"FIVE MASSIVE DATA BREACHES AFFECTING SOUTH AFRICANS"

Per Fin24.com June 19, 2018

IN AUSTRALIA:

"THE LAST QUARTER OF 2018 SAW MORE AUSTRALIAN DATA BREACHES THAN EVER"

Per CSO Magazine February 7, 2019

IN ASIA PACIFIC:

"ASIA PACIFIC IS NO 1 HUNTING GROUND FOR HACKERS"

Per E Hacking News March 5, 2019

IN EUROPE:

"OUT OF THE NUMBER OF DATA BREACHES REPORTED IN EUROPE BETWEEN MAY 2018 AND JANUARY 2019, BY COUNTRY. NETHERLANDS RANK FIRST WITH OVER 15,000 CASES, WHILE THE DATA BREACHES REPORTED TO THE GERMAN AUTHORITIES AMOUNTED TO 12,600."

According to Statista





Is ISO/IEC 27552 the Answer to Meeting Privacy Needs?

In my opinion, ISO/IEC 27552 as an extension to ISO/IEC 27001 and ISO/IEC 27002 is a good tool in the quest to keep ahead of breaches and to stay compliant with all of the worldwide requirements, some of which are mentioned in the opening paragraph. My perceived challenge in using ISO/IEC 27552 is the need to continuously refer to ISO 27001 and ISO 27002 as the reader is directed to specific clauses in these two standards. That being said, the standard does give a lot of additional guidance related to privacy not found within ISO/IEC 27001 and ISO/IEC 27002, making the effort worthwhile.

ISO/IEC 27552 can be easily fit into the Information Security Management System (ISMS) defined in ISO/IEC 27001. ISO/IEC 27552 defines additional requirements and provides guidance for protection of privacy and when coupled with ISO/IEC 27001, they constitute a Privacy Information Management System (ISMS), which closes a lot of gaps in the attempt to have a functional Information Security Management System in place, and at the same time comply with data privacy regimes, such as the GDPR.



About the Author

Michael C. Redmond, PhD
Director of IT & GRC Consulting and Audit for EFPR Group

Michael is the Director of IT & GRC Consulting and Audit for EFPR Group, an International Consulting and Audit Firm. She teaches Lead Auditor and Lead Implementer courses for PECB. She has an MBA in International Business and Marketing from Fordham University and is currently completing her MBA in Risk Management at PECB University, and plans to start an MBA in Information Security with PECB University upon the completion of the current one. Michael has also successfully published two books: “Mastering Your Introduction to Cyber Security” and “Mastering Business Continuity Management; Mastering Your Work Life Balance”.


16
91



BRUSSELS

Europe's Heart has it all. It's an art canvas, a time-travel machine and a food lovers' paradise.

Brussels is a fairly small city, so you can visit a lot of exciting sights even if you have planned a short trip. The architecture is beautiful, there's a lot of green space, and the chocolate, waffles, fries, and beer will have you never wanting to leave! Brussels is the center of numerous architectural wonders and world-heritage sites.



Transportation

Brussels has an extensive public transportation system and the city center of Brussels is accessible by trams, buses, and metro lines. A single metro ticket costs €2.10, and a 24-hour ticket costs €7.50. You can also get the MOBIB card (transport tickets of the four Belgian public transport operators). A 3-day pass for less than €10 can be used for all modes of public transport. Taxis are another transportation option, and the most expensive one.

Accommodation

Brussels provides a variety of accommodation options, from budget to mid-range and luxury. Some luxury options that are mostly used during business trips and conferences are:

Brussels Marriott Hotel Grand Place

The location is ideal - most of the central attractions are at walking distance. It is less than a 7-minute walk to the Grand Palace and about 10 minutes to the Royal Museum of Fine Arts of Brussels. There is also a subway station at the corner. Plus, there are plenty of restaurants around, so you will find yourself in the middle of everything.

The Dominican

The hotel is beautiful and modern and is centrally located, less than a 5-minute walk to many of the key locations, such as the royal galleries and the Grand Place. The metro station is in a distance of 100 meters and there are many restaurants around.



A Belgian Taste

Belgian cuisine is widely diverse, with significant regional variations while also reflecting the cuisines of neighboring countries. Belgium is best known for its chocolate, waffles, fries and beer. To eat authentically, and enjoy the most classic dishes you should definitely try some of these foods:

Moules frites: One of Belgium's national dishes and a popular choice. Mussels and fries are symbols of Belgium's gastronomy. Mussels are prepared in large steaming pots and coated with a white wine sauce and sprinkled with fresh herbs and vegetables. They are accompanied by a bowl of Belgian fries and homemade mayonnaise.

Filet Américain: This is basically a raw steak that has been chopped in small pieces with very sharp knives and marinated with onions, capers, Worcestershire Sauce, an egg yolk (the French word is: Steak Tartare. The preparation might differ a bit from place to place).

Chicon (or Witlof in Dutch): It is a root of chicory that has been growing in a warm cellar, away from all light. It can be eaten raw or cooked (the water is replaced after a few minutes so the root is not bitter), and they are often used in salads or served raw.

Potatoes: No Belgian plate would be served without potatoes. There are 3 museums of potatoes in Belgium. I prefer small potatoes that are quickly cooked in water with their skin on and then cooked in a pan with butter or with the fat of the meat you will be eating them with.

Eel in the Green: Even though less frequent nowadays, it is a real delicacy, and it was available to everybody a bit lucky to grab one.

Asparagus: Preferably the white ones as they are local (I prefer the green or the wild ones). Dipped in boiling water for not too long, and they are ready to eat.

...and finally, **French fries:** do I have to explain? Our traditional fries are cooked twice in beef fat (don't tell your PR, he will choke).

This has been institutionalized to even qualify for the Best Fritkot (every village had a person selling French fries from a refurbished caravan). If you think I am joking, you can read more here. In the 1980s, it was not uncommon for bands to head off to one of those renowned Fritkot & queue-up after their concerts, like anybody else. The urban legend mentions Toto's, AC-DC, The Rolling Stones.

Where to find all those simple meals?

If you are in the Brussels city center, you can always go to the long-standing brands which should not deceive you. Close to the city center you have "Rue des Bouchers" (Butcher's Street). It is commercial but you should not have any problem getting a nice "Moules Frites" (Mussels and Chips) at **Chez Léon.** Chez Léon is the place to go for this traditional Belgian dish. The decor and atmosphere are unique, with excellent food and service. Put it on your itinerary if you are visiting the city, but get there early if you want to get a place.

Close by you have the **Taverne du Passage.** It is nothing fancy, but it is a brasserie-like set up with all the "simple" meals served with plain quality. You can easily locate it on Galerie De La Reine (Queens Gallery). It's a place with an old-style setup but with delightful modern cuisine.



Belgian cuisine was definitely inspired by the French cooks. Numerous regional meals still hold a good place on the menu according to regional preferences.



Finally, I would propose you to go over a few places in the city center, like the cafe where there are 1200 beers available on the menu (and in the cellar) or just one of those old-style cafes like:

La Mort Subite. You step into a little piece of history when you enter this bar – the décor is authentic, and it hardly has changed since it opened in 1928. The place keeps the touch of history and offers a fantastic range of local beers. Definitely worth a visit if you're at the center of Brussels.

Belga Queen. Close to the city center you can also find this fantastic place. It is the building of an old bank that has been converted into a restaurant. It is usually very good quality in a very nice building. It is a warm place for a coffee or for a happy afternoon drink. During the week there is always something going on but it still has plenty of space. In the weekend it is packed though.

Restaurants

If you really want to go for the first-class exuberance, I can recommend you **Bon Bon**. It is pricey, but you get the best of the best. Tables are booked up to a month in advance. Creativity is the hallmark of this restaurant - and no compromises are made with the quality of the food. The dishes are like paintings on a plate. The staff is very attentive and friendly, which gives the restaurant a nice and relaxing atmosphere. It is in a lovely villa on the Avenue de Tervueren with easy access and designated parking - a great experience indeed. Ranked in the top of the tops, Bon Bon is given 19,5 / 20 by Gault & Millau, while Michelin gives only 2* as they require several positive evaluations before giving another star.

Among the more traditional restaurants, there is **Comme Chez Soi**, which was the world #1 according to "Gault & Millau" and Michelin in the 1990s. This is an amazing restaurant with impeccable service. The food is true art in this restaurant, with so much detail in every course. Everything is seasoned and cooked to perfection to give a wonderful array of tastes and flavors.



And of course, you should not miss the **Cantillon Brewery.** It is conveniently located on Rue Gheude in the Anderlecht district. To get more insights you have the chance to take the self-guided tour which costs €7 (full-guided tours are also available), and a member of the team gives you a talk through the history of the beers, how the beers are prepared, different beer types, etc., and then you are allowed to do your own tour of the brewery building, which is awesome - there is so much to see and learn. At the end of the tour, you are entitled to taste two different beers of your choice in the cool brewery bar.

...and the famous chocolates & waffles

You probably have all heard of Belgian chocolate and waffles. For chocolate lovers (but let's be honest, who doesn't like chocolates) there are multiple chocolate tasting tours and workshops on offer. I suggest you visit the **Choco-Story Museum** if you want to learn more about the history of chocolate. This museum, apart from the exhibition of the history of chocolate gives the visitors a chance to see how chocolate pralines are made.

One of the best chocolatiers is **Pierre Marcolini.** Marcolini has his own cacao plantations and uses only the best for his creations. You can tell the craft and dedication put into these chocolates. When you try them, you can tell why Belgium is famous for chocolate. They also wrap the chocolates beautifully, and they make for a beautiful gift!

Another delicacy that characterizes Brussels is Belgian waffles. Available at every corner of the city, airy and with a melt-in-your-mouth texture, you are able to indulge yourself with a variety of toppings, such as ice cream, whipped cream, powdered sugar, chocolate, and fruits. One of the best places for waffles is **Maison Dandoy** - absolutely delicious waffles! You need to be aware that there is always a long queue (which is always an indication that the place is nice). However it's worth the wait.

Attractions



The Grand Place. The Grand Place is definitely a place you want to visit when you are in Brussels. It is a special gem of history, architecture, cultural and traditional activities, nativity scenes during Christmas, flower carpets, nice restaurants and shops. Also, be sure to see the Grand Place at night. It is very pretty under the magic of the carefully designed lighting. Once every 2 years, they make a massive flower carpet with nearly 1 million begonias in less than 4 hours.



The Strépy-Thieu Funicular Lift. One of the must-do experiences is The Strépy-Thieu Funicular Lift, 50 km outside of Brussels. It is a brilliant piece of engineering and is an absolute must-see. You can also visit the engine room, and this would be worth a visit before boarding the boat. There's a viewing gallery on the fifth floor and an exhibition on floor eight. The accompanying video (English audio guide available) is extremely interesting and describes how the lift came into being. The trip includes a visit to the engine room of the old lock to see it run and a mini train trip back to the Strepy-Thieu Funicular Lift where you can go inside and find out about the construction of this amazing boat lift. The boat trip lasts 2-2.5 hours including a visit to the machine room.

Atomium. The unavoidable icon of Brussels is the Atomium. As you approach the Atomium, I assure you that you will be in absolute astonishment by its appearance. Even though not all Atomium spheres can be visited (more precisely, the three outer spheres that are below the top one), there is still a massive number of visitors, interesting facts as well as a light show inside the rest of the spheres. It is recommended that you also visit the restaurant at the top, where they serve a range of reasonably priced snacks and drinks - The view is spectacular. The park near the Atomium is also a nice place to visit.



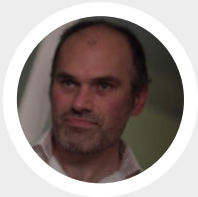
Musical Instruments Museum (MIM). The MIM has a very comprehensive collection of musical instruments including mechanical instruments in a splendid building. You have multiple floors of displays and you can get really close to instruments of every era. The point is that the old instruments have been carefully maintained and can be played, but not by visitors. The museum has audio guides playing samples of the rare instruments. There is also a lovely gift shop, with very interesting gifts. The rooftop restaurant offers a magnificent view.

Brussels was one of the birthplaces of the Art Nouveau movement. There are several walks that go around the town to view several of those houses (of course, you cannot visit them in most cases but you can admire the façade). Brussels is a significant center of Art Nouveau and home to prominent architects. These architects used the facades of their buildings as spaces for endless experimentation. Next time when you find yourself walking down the streets, make sure to walk through these distinct architectural gems: the Art Nouveau houses of Brussels.

Another interesting walk would be in the "low" end of Brussels where there is a display of amazing graffiti. There are several that were made by very famous artists. Also, you should not miss visiting the Royal Theatre Toone pub in Butcher's street, where they have a marionette show. After the show is finished you can have some beer and food in their pub, which is also full of puppets and has a magical atmosphere. You must reserve if you want to see a show because they are booked months in advance.

Brussels offers much more than I could present in this article. I suggest taking your time to explore and maximize the time, even if it's a short trip. Brussels offers its visitors several activities and experiences, from magnificent sights to delicious food.





About the Author

Thomas Lionel Smets
Security Consultant / Security Designer

After graduating in Physics, Thomas worked for several years in a bank before moving to pure IT companies as a Java Developer. After 8 years as an employee, Thomas became a freelance professional but kept on doing similar jobs – always with a keen interesting in release management. Usually on long assignments, he specialized in IT Security while doing PM work. After getting the CISSP & several other certifications, Thomas is now contracting SMEs while giving Cybersecurity trainings 5-10 times a year. Thomas is also an active Rugby coach in the Kituro Rugby Club & an occasional Rugby referee.



An Analysis of the Upcoming NIST Privacy Framework

BY PECB

"The world is more interconnected than ever before" – an expression that has become so common that it's safe to say it has reached the cliché status. Nevertheless, whether one is annoyed by this expression or feels sympathetic toward it, he or she cannot deny its truth. The rapid advancements in information technology from the 1990s onwards, have given individuals an unprecedented degree of comfort, and businesses a remarkable opportunity to operate swiftly and create enormous economic value. To a large extent, it is the data provided by individuals that serves as fuel to this data-driven and information-hungry machine. At any given point, there is a gargantuan amount of data being moved from a server to the other.

What makes privacy matters more complex is that the movement of information is often not confined within the borders of a single country but is scattered among multiple parts of the world, where views on privacy are different, and the laws and regulations to enforce privacy protections vary.

However, as individuals interact with the systems, products, and services that businesses offer, and are more or less voluntarily sharing their private information, it has become increasingly difficult for them to understand the impacts or deal with the potential consequences regarding their privacy that come as a result of this interaction.

Throughout the world, governments and independent organizations have taken measures and are launching initiatives to tackle these privacy challenges. The European Union, for example, which has the right to privacy enshrined in its Charter of Fundamental Rights (Article 7, "Everyone has the right to respect for his or her private and family life, home and communication") has created the General Data Protection Regulation (GDPR), which aims to offer data protection and privacy for all EU and EEA individuals and citizens.

On the other hand, at the non-governmental side, ISO has published ISO/IEC 29100, which provides a privacy framework applicable to any system or service that requires Personally Identifiable Information (PII) processing. Furthermore, ISO is also working on adding ISO/IEC 27552 to its highly successful ISO/IEC 27000 family of standards. This standard is currently under development and it specifies requirements and provides guidance for establishing, maintaining, and continually improving a Privacy Information Management System (PIMS) as an extension to an ISMS based on the requirements of ISO/IEC 27001 and the guidance of ISO/IEC 27002.

In the United States, the National Institute of Standards and Technology (NIST), a non-regulatory agency of the U.S. Department of Commerce, is currently developing a voluntary privacy framework. According to NIST, this privacy framework can help organizations answer the fundamental question:

"How are we considering the impacts to individuals as we develop our systems, products, and services?"



This privacy framework is going to be an enterprise risk management tool for organizations to help them consider:

- How their systems, products, and services affect individuals and,
- how to integrate privacy practices into their organizational processes that result in effective solutions to mitigate these impacts and protect individuals' privacy.



Among other objectives, through this privacy framework, NIST aims to establish a common taxonomy that is neither country, nor region specific. By doing this, NIST allows organizations inside and outside the United States to use it for strengthening their own privacy efforts, while at the same time, contributes to developing a common language for international cooperation on privacy.

Why Cybersecurity alone is not enough?

In 2014, NIST published the Framework for Improving Critical Infrastructure Cybersecurity (commonly known as Cybersecurity Framework). Since its release, this framework has helped many organizations communicate and manage cybersecurity risks. As NIST states, these risks arise from "unauthorized activity related to the loss of confidentiality, integrity, or availability of a system or information asset."

However, privacy risks do not occur only as a result of the actions of those with malicious intents. The authorized data processing can also lead to unintended or adverse consequences for individuals.

Businesses, for example, when providing services and marketing products, can use individuals' information in ways that increase their vulnerability



to fraud and identity theft. This can have a profound effect on the lives of many individuals. Thus, as stated by NIST, unlike cybersecurity risks, privacy risks arise as "a byproduct of intentional (i.e., authorized) data processing occurring in systems, products, and services that help organizations to achieve their business objectives."

The NIST Privacy Framework components

The aim of this Privacy Framework is to improve privacy risk management between business/mission drivers and privacy protection activities. It is intended for organizations that use data processing systems, products or services irrespective of their sector, focus or size. The NIST Privacy Framework consists of three components: the Core, the Profiles, and the Implementation Tiers.

The Core is a set of privacy protection activities and preferred outcomes, consisting of five simultaneous and continuous functions, which together provide a high-level and strategic view of the privacy risk management of the organization. These functions are "Identify, Protect, Control, Inform and Respond", and all of them consist of key categories and subcategories. The Core functions should not be seen as sequential steps to an end state. Additionally, they are effective when performed concurrently and continuously. Functions, categories and subcategories work closely to properly address the privacy risks. The five functions organize the basic privacy activities, where the Identify, Protect and Respond functions can also be used by the Cybersecurity framework for privacy risk management. The categories segment a function into groups of privacy outcomes related with programmatic needs and activities. Likewise, subcategories divide a category into outcomes based on technical and management activities that need to be implemented.

The draft version of the NIST Privacy Framework: "An enterprise risk management tool" has 5 functions, 23 categories and 111 subcategories as presented in the Appendix A: "Privacy Framework Core".

The Profile: The organization establishes a profile in accordance to the functions, categories and subcategories with the business requirements, risk tolerance, privacy values, and resources of the organization. The approach that the Privacy Framework risk-based approach takes, is allowing the organization to tailor the functions, categories and subcategories to its specific needs. This risk-based approach also allows them to take into account new additional functions for unique risks that the specific organizations may face. Profiles are utilized to create a clear picture of the current state of the organization as well as what is the desired target state. This makes it possible to distinguish the privacy outcomes that the organization currently achieves and those that it plans to achieve.

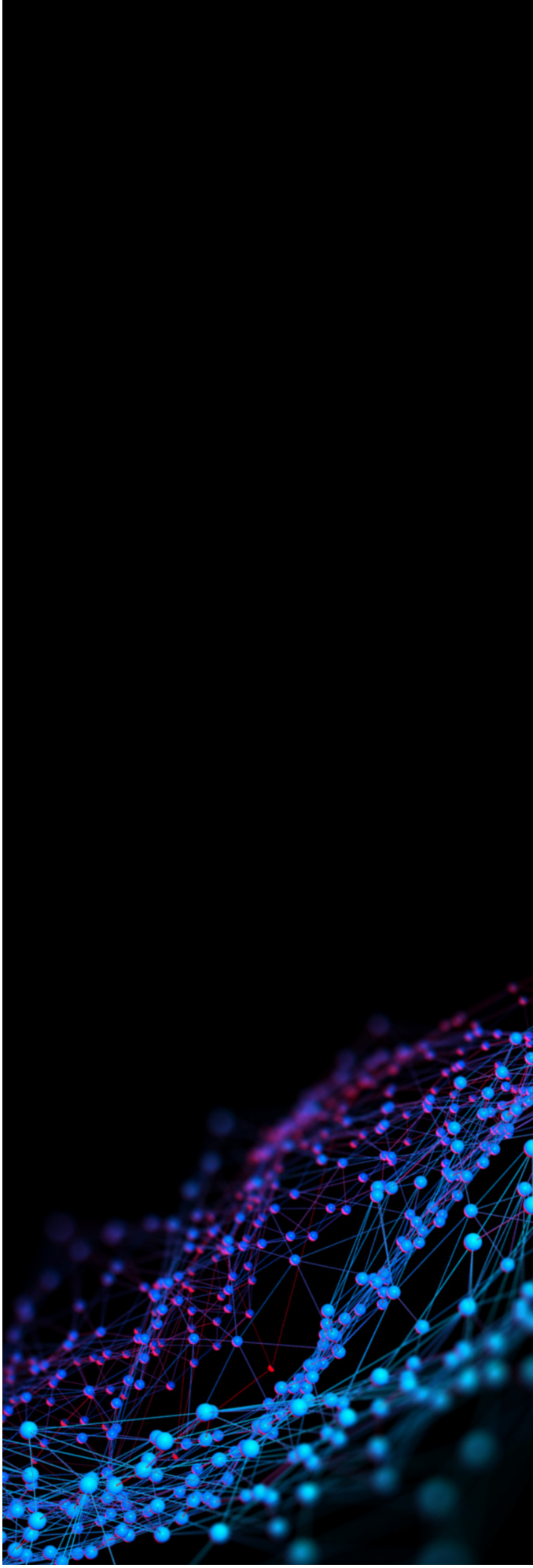
The Implementation Tiers help organizations manage privacy risk by considering the nature of such risks and the competence of processes and resources in place. There are four types of tiers known as Partial — Tier 1, Risk Informed — Tier 2, Repeatable — Tier 3, and Adaptive — Tier 4. Tier selection affects the Profiles and the privacy risk management within the organization. Thus, before selecting the tier, organizations should consider their current risk management practices, data processing systems, products and services, legal and regulatory requirements, privacy needs of individuals, etc.

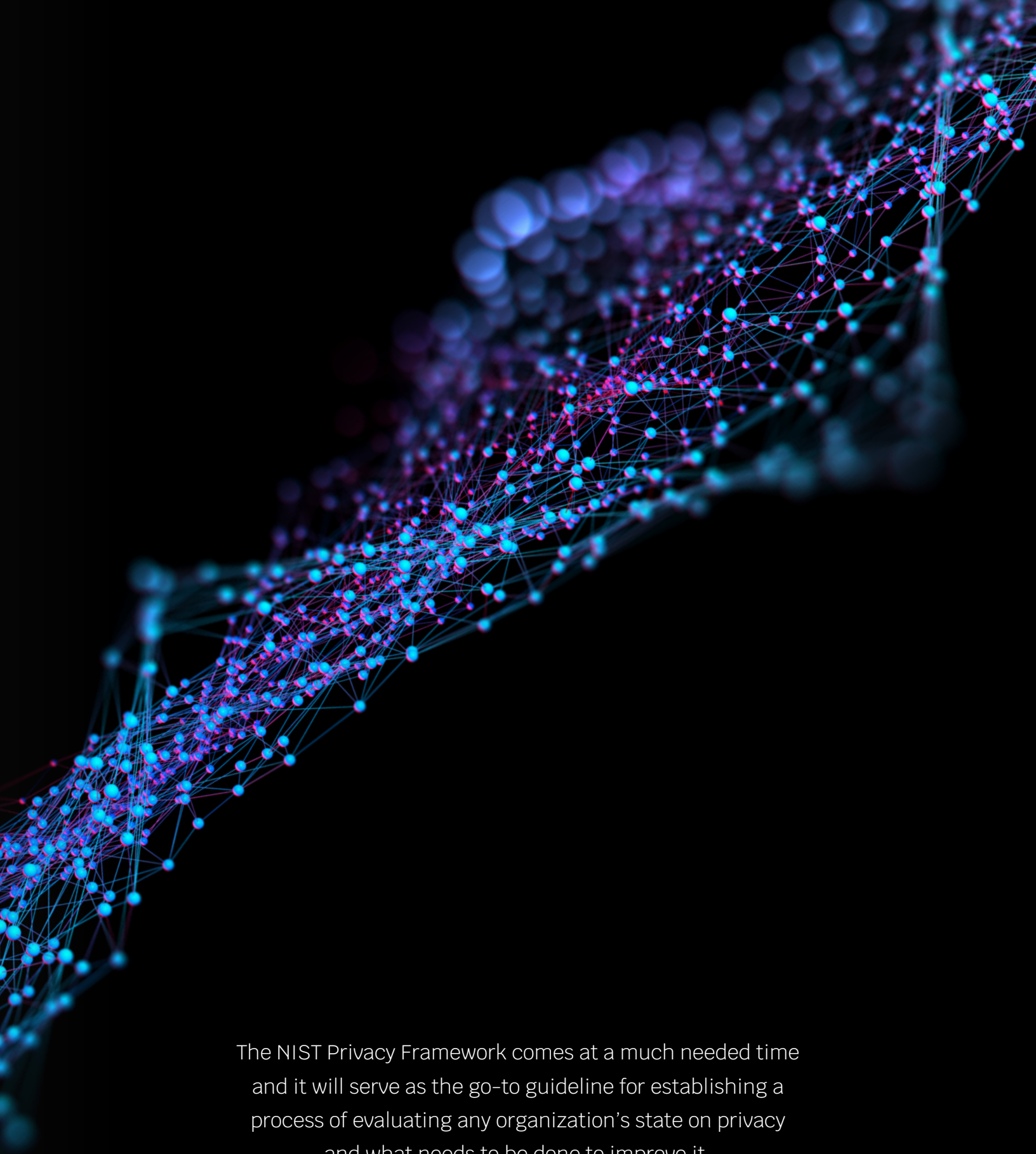
How to use the Privacy Framework?

The Privacy Framework supplements the existing development operations, articulates privacy requirements to partners and customers and supports the identification of gaps in the organizations' privacy practices. It is up to the implementing organization how to use the Privacy Framework. Organizations can use the subcategories in the Core and map them with specific sections of regulations, standards, guidelines and practices in order to support the further development of systems, products and services by taking into consideration the individuals' privacy needs.

Moreover, the Privacy Framework can be used to compare the existing privacy activities with the activities of the Core. The Current Profile helps an organization analyze the level of outcomes achieved and determine if it needs an action plan to build up the existing privacy practices and minimize privacy risk.

The Privacy Framework helps create a new privacy program or enhance the existing one by using the "ready, set, go" phases. For an organization, it is essential to understand its business environment and the privacy risks of its systems, products or services and then conduct a privacy risk assessment using the Identify function. Then, the organization can set an action plan based on the comparison between the Current Profile and the Target Profile. In order to reach the Target Profile, the organization should adjust its existing privacy practices.



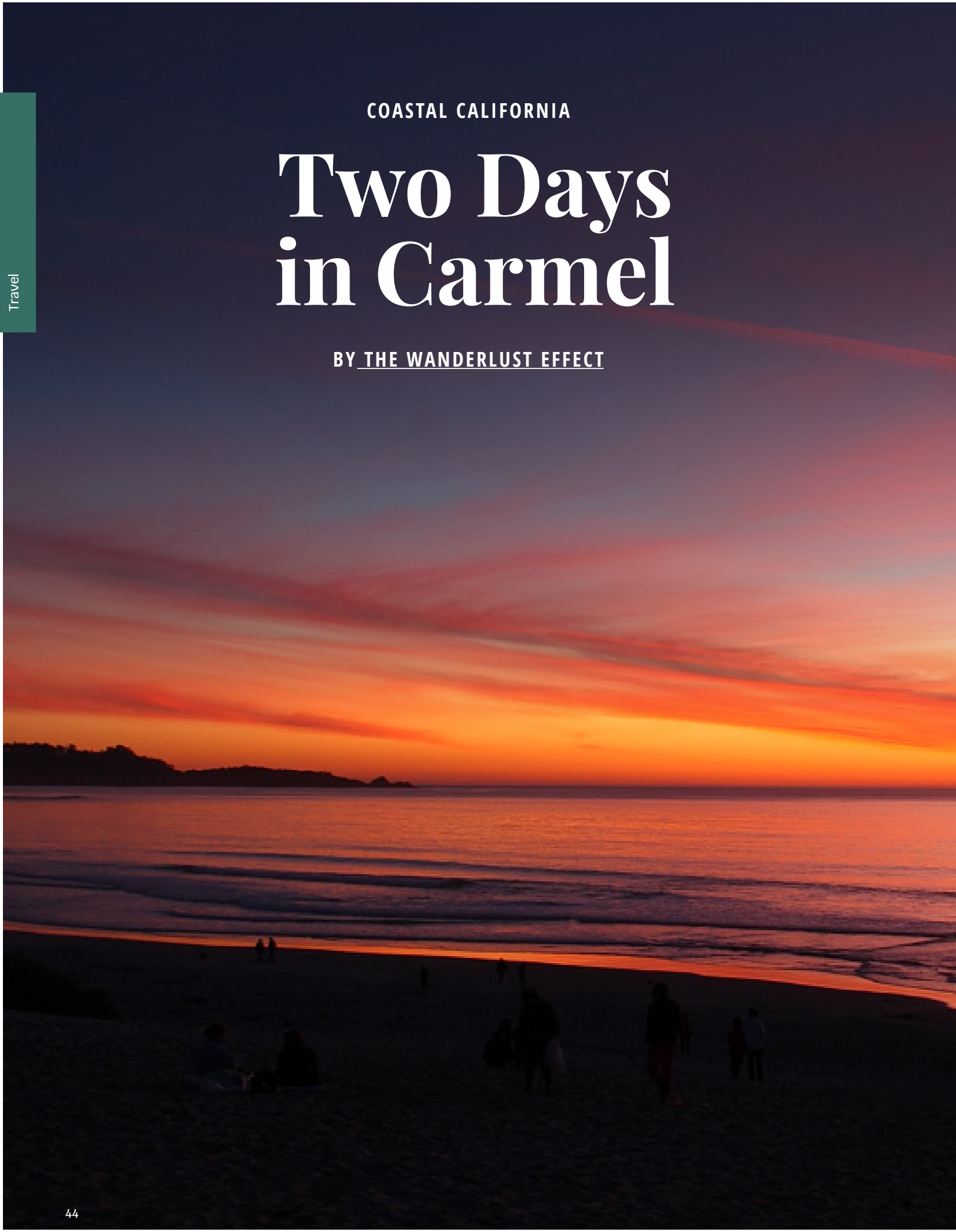


The NIST Privacy Framework comes at a much needed time and it will serve as the go-to guideline for establishing a process of evaluating any organization's state on privacy and what needs to be done to improve it.

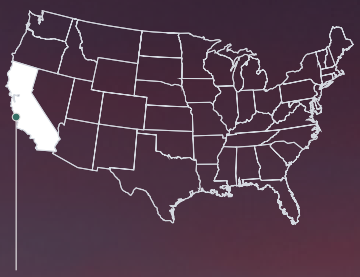
COASTAL CALIFORNIA

Two Days in Carmel

BY THE WANDERLUST EFFECT



Visits back to California are generally few and far between for us, and when we booked a return to California in December, we added on a few days so we could create some more memories in our home state. One of my favorite seaside towns in California is Carmel, a picture perfect little enclave that's the perfect coastal retreat for a romantic escape, a family adventure, or a girls' getaway. We booked two days in Carmel to spend with my family for a couple of days of R&R in one of California's most stunning coastal towns.



CARMEL, CA

FLICKER/GREENJACKET88

DAY 1

Explore Carmel-by-the-Sea









FLICKER/GREENJACKET88

In a town where there are no physical addresses, a famous former mayor, no chain restaurants, and a permit required to wear high heels (legitimately!), you know you're going to be in for charm overload and Carmel doesn't fail to deliver. The experience of Carmel is multi-faceted and while it's on the water, I find the ocean itself to be a secondary draw (though some may disagree with that). To me, it's the town itself, dotted with independent boutiques and cute restaurants that keeps me coming back.

Brunch in Carmel

One of the things that surprises us a bit with Carmel is the lack of seaside dining. You'll find that places for breakfast, lunch and dinner are in town, not on a waterfront stretch with a view. I'm not sure if this has to do with building codes, but it feels like a major missed opportunity for that sunset/happy hour period when you could easily enjoy a glass of wine and some oysters overlooking the Pacific; anyone else with me?! That all said there's plenty of lovely dining in town and a number of cute places — my favorites include The Cottage and Village Corner. This year we had breakfast at Carmel Belle, which we enjoyed too though it's a bit further from the seafront. Fuel up because you have a day of walking and shopping ahead!



Boutique Hopping

Carmel is a shoppers' haven, with quaint boutiques and upmarket shops lining the main thoroughfare from Junipero Street down the seafront. At Junipero and Ocean Avenue, you'll find Carmel Plaza with a slew of familiar shops, plus a few pleasant surprises like the Cheese Shop, which is absolutely heaven for cheese lovers (they also have wine if you're looking to grab a few things for a picnic). Ocean Avenue is the main artery of Carmel-by-the-Sea but the side streets also have fabulous shopping so be sure to wind your way through town!

Wine Tasting

While places like Napa Valley, Paso Robles and Temecula may come to mind when you think of wine tasting in California, quaint Carmel has a little scene of its own in the form of tasting rooms! Instead of visiting vineyards, you can incorporate wine tasting seamlessly into your two days in Carmel, whether you're looking to dedicate an entire day to it or just to weave it in to a broader itinerary. Carmel's Wine Walk by the Sea pinpoints tasting rooms in town – there are many! So you can plan accordingly.

If you're planning on making wine the focus of your two days in Carmel (or longer!), consider purchasing the Wine Walk's "Passport", which grants you a wine flight at 10 of the 13 tasting rooms.

Beach Glimpses

I mentioned this above, but Carmel is interesting to me because it's a town where the beach happens to be part of the landscape. There are some cities where the beach is the reason for your getaway, but that's not really the case in Carmel. The seaside component is part of the draw but unless it's particularly sunny summer day, you probably won't find yourself laying out on the beach. That all said, it's a beautiful stretch of coastline and your stroll down Ocean Avenue will have you bumping right into the beachfront. There are perches for viewing or you can take a picnic and enjoy lunch with a view.

Dinner in Carmel-by-the-Sea

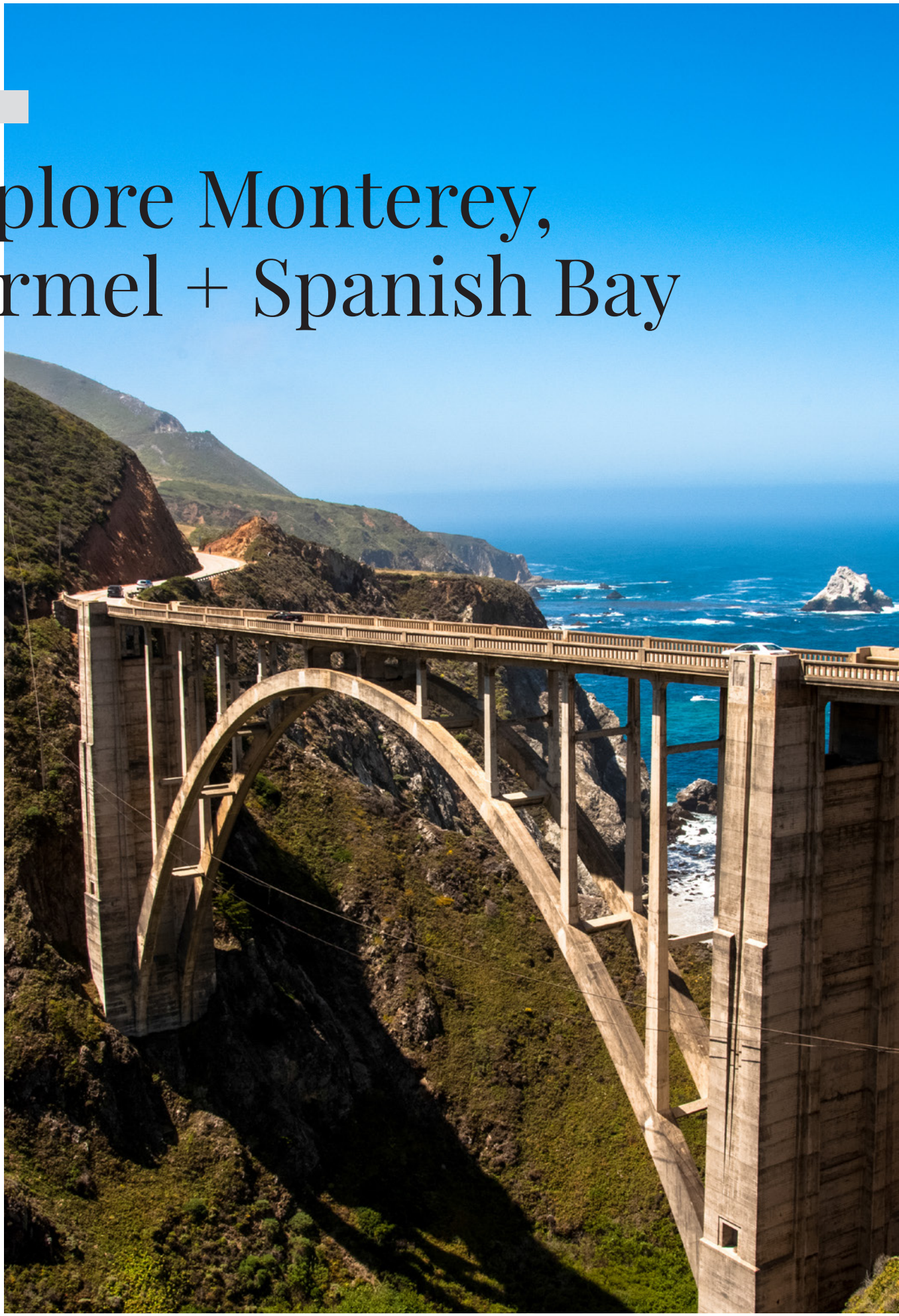
End your day with dinner in Carmel with your choice of a number of highly rated restaurants. If you want to venture a bit further afield, Carmel Valley (about 15 – 20 minutes away) has a number of options as well. In Carmel-by-the-Sea, we loved Cultura for a cool vibe, great regional Mexican cuisine, and fun tequila and mezcal-inspired cocktails. For a post-dinner drink (or pre-dinner!) head to Brophy's Tavern for a polished pub setting.





DAY 2

Explore Monterey, Carmel + Spanish Bay






FLICKER/LOLLYKNIT

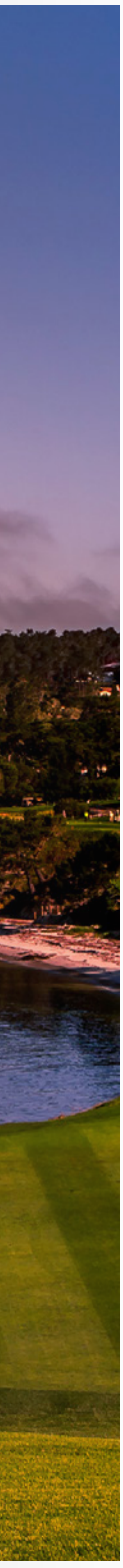
During the second of our two days in Carmel, we opted to spread the love and enjoy some of Carmel's photogenic neighbors as well. You could easily spend another day in Carmel doing the same as the first: shopping, wine tasting, lazing, and enjoying the town's beauty, and it would be an absolutely perfect day. If you're more into exploring and want to venture a bit, our day two covers some inspiration for the explorers out there.

Spend the Morning in Monterey

I'll be honest with you: in my memories, Carmel always far exceeded Monterey. I always preferred the polish of Carmel's facades and the upmarket feel of the town. I had mentally downplayed Monterey's charm for a long time. My grandmother, who joined us on this trip, had fond memories of long leisurely drives down to Monterey where she and my grandpa would enjoy a seaside lunch before heading back up north so we recreated that with a morning in Monterey, which is about a 15 – 20 minute drive from Carmel. We started the day exploring the shops at Cannery Row, popping in as some of the first visitors of the day while the town was coming alive. Monterey feels a bit more kitschy than Carmel so expect shops to generally slant a bit more touristy than chic (there are still some good ones in the bunch).

Here's one way that Carmel differs from Monterey: while you'll be hard pressed to find seaside dining in Carmel, it's everywhere in Monterey. I say that to say, enjoy lunch with a view! We did lunch at Schooners, which is enclosed (good for chillier days) but still offers a lovely view of the Pacific. I've been to Monterey many times in my life so have fortunately seen many of the 'must-sees' in town but if it's your first ever trip, you should also visit the Monterey Bay Aquarium. With a $50 entry fee, it's not an inexpensive endeavor so you'll want the time to allocate to fully enjoy it — it's truly one of the most impressive aquariums you'll see!





Afternoon in Carmel

If you're back from Carmel for the afternoon, you'll basically be recreating your first day! I could spend a few days exploring the shops and wine rooms in Carmel. There really are more shops than you'll be able to take in during a single day. For luxury seekers with champagne taste and more of a prosecco budget, check out Foxy Couture on San Carlos & 7th Ave. For vintage luxury finds from clothing and shoes to handbags and accessories.

Drinks at Spanish Bay

It's hard not to think about the epic golfing on the Monterey Peninsula, and with the world-class courses come beautiful lodges, upscale spa experiences, and lovely restaurants for visitors to enjoy. We opted to take an Uber (about 15 – 20 minutes) instead of driving and headed to Spanish Bay to settle in for sunset to enjoy a cocktail while listening to the bagpiper on the greens. It gets chilly at night by the coast so even in summer, plan on bringing something to bundle up. The course provides blankets for visitors (thankfully) and the fire pits are the perfect place to thaw out once the sun has gone down.

Where to Stay in Carmel

Lastly, let's talk where to stay in Carmel. To me, a boutique property is what you're looking for to enjoy Carmel's quaint quality, and location my absolute #1 criteria because Carmel is a place that's designed to see on foot. Staying too far outside of a comfortable walking radius will just have you wishing you'd picked something central. A few good options: Vagabond's House Bed and Breakfast Inn, Carmel Country Inn (pet friendly), Tradewinds Carmel, and L'Auberge Carmel, a Relais & Chateaux property. If you're traveling with family or a small group, consider looking to Airbnb for great alternatives in the heart of town. We rented a three-bedroom home – Chateau by the Sea – on Ocean Avenue in Carmel, which we adored. It exceeded expectations in a major way, giving us the comforts we needed (plus a dose of luxury!) without having to worry about securing multiple hotel rooms.







THE VENUE FOR NOTEWORTHY INSIGHTS

Mark your calendar! In this year's PECB Insights Conference we will be presenting a new format, which will consist of a series of roundtable discussions. This new format will make the conference more interactive and provide attendees with a valuable chance to network. The topics which will be explored and discussed have been chosen to provide attendees with an in-depth knowledge on Information Security and Risk Management.

When choosing the topics for the conference there was a specific focus on incorporating the changing and continuous advancement of technology and its impact on businesses functions. For this reason, the topics are inclusive of various issues and benefits of new technologies and how they could potentially have an impact on existing frameworks and policies. These selected topics will provide attendees an opportunity to learn about the impact of AI technology, Blockchain, IoT, and the effects that these will have on their organization and organizational procedures.

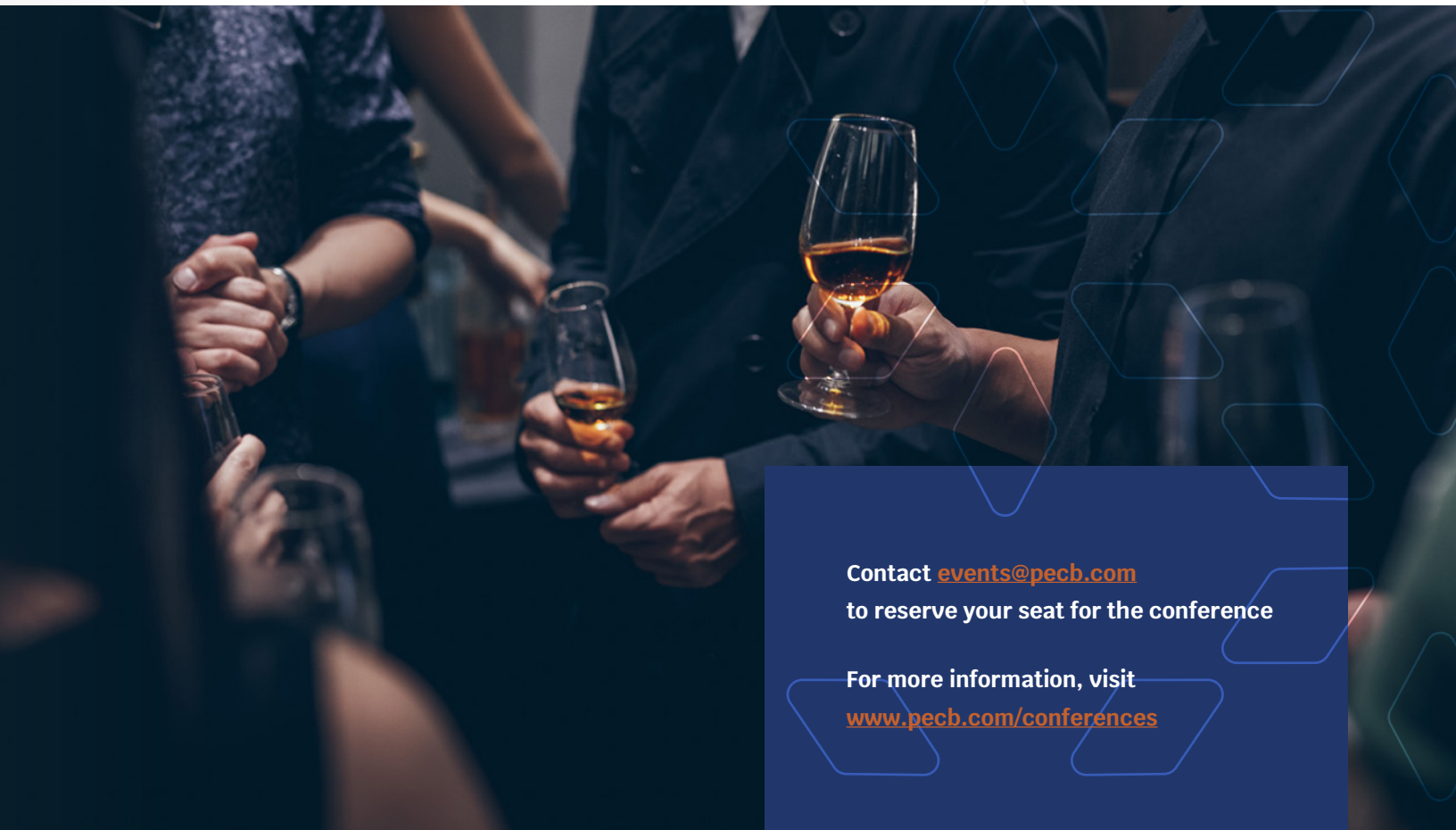
This year, the conference theme is **Information Security & Risk Management.** These topics will be explored and discussed by more than **50 panelists** in order to provide attendees with in-depth knowledge and insights.

In addition to recent trends and technological advancement, there will also be a focus on issues of cybersecurity, where case studies such as the Facebook and Twitter breaches and the lessons learned from these events will be discussed. The discussions will explore the issues and solutions for these cyber security threats and tackle issues such as the shortage of cybersecurity talent. There will also be a focus on data protection and how effective data protection regulations have been so far. Attendees will have the opportunity to find out how effective companies and organizations have been in complying with the General Data Protection Regulation (GDPR) a year since its implementation – this will be discussed both in English and French. Take a look at the official agenda to see the topics that have been selected for this year's conference.

THE PECB GALA NIGHT

The PECB Gala Night will be held on October 3, 2019, and will include a full-course dinner and cocktails, with a special entertainment surprise. This is a perfect opportunity to network in a more casual setting, and make long lasting connections. Moreover, during the dinner, guests will be able to interact and witness the global presence PECB has created. With Partners from across the globe, this is the ideal occasion to create connections from every corner of the world. The gala night is a special night, where PECB will be celebrating the hard work and dedication of its global network. With an awards ceremony dedicated to our Partners, Trainers and Auditors, guests can witness the appreciation PECB has for their commitment.

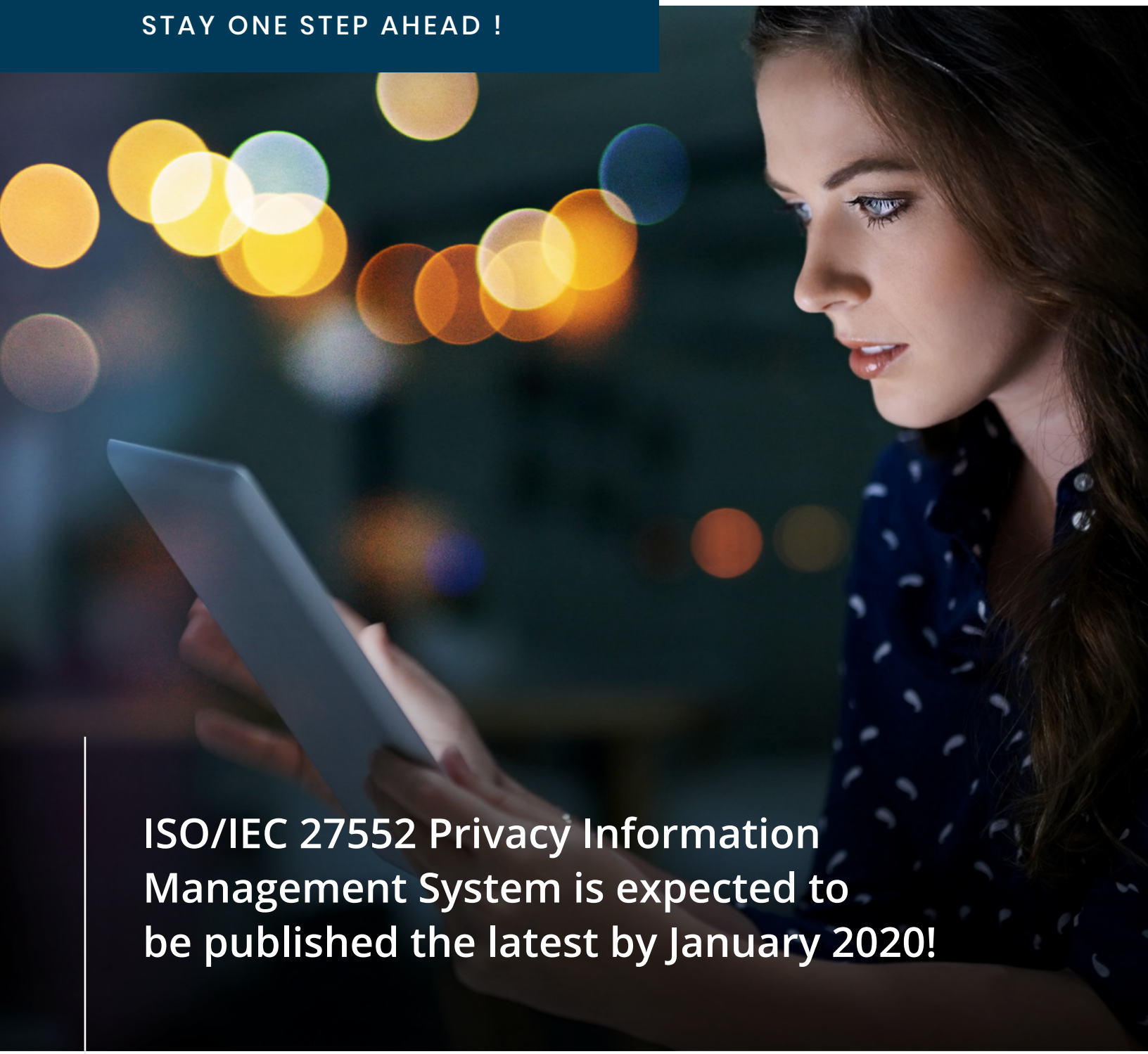
Make the most out of your trip to Brussels by taking one of our Pre-Conference training courses. The training courses will start on September 30 and end on October 2, 2019. This year, the two courses to choose from are ISO/IEC 27552 Lead Implementer and PECB Certified Management Systems Auditor (CMSA).



Contact events@pecb.com
to reserve your seat for the conference

For more information, visit
www.pecb.com/conferences

STAY ONE STEP AHEAD !



ISO/IEC 27552 Privacy Information Management System is expected to be published the latest by January 2020!

The standard which provides requirements and guidelines for the implementation of a Privacy Information Management System is currently under development.

ISO/IEC 27552 will allow organizations to use a single set of controls to comply with multiple privacy regimes, such as the GDPR. It will be of great interest to any organization with an ISO/IEC 27001 ISMS already in place.

Keep updated on ISO/IEC 27552 developments by subscribing to our newsletter!



Do you want to know what it is?
Stay updated by subscribing to our newsletter.



BEYOND TRADITIONAL EXPERIENCES!

Redefine success and enrich your career.

Course	Language	Status	
ISO 21001 Lead Auditor	English	New!	›
ISO/IEC 27032 Lead Cybersecurity Manager	Latvian	New!	›
ISO/IEC 27002 Manager	Czech	New!	›
ISO/IEC 20000 Lead Implementer	English	Updated	›
ISO/IEC 20000 Lead Auditor	English	Updated	›
ISO 22000 Introduction	English	Updated	›
ISO 55001 Lead Auditor	English	Updated	›

BECOME A PECB CERTIFIED MS AUDITOR AND ADVANCE YOUR PROFESSIONAL CAREER IN AUDITING!

Challenge your limits and expand your goals by attending one of our upcoming Certified Management Systems Auditor training courses.



PHILIPPINES
September 10-12, 2019
southeast.asia@pecb.com



NIGERIA
September 23-25, 2019
africa@pecb.com



SENEGAL
September 23-25, 2019
francophonie@pecb.com



MOROCCO
October 1-3, 2019
francophonie@pecb.com



STOCKHOLM
October 3-5, 2019
anders.carlstedt@pecb.com



MALAYSIA
December 9-11, 2019
asia@pecb.com



DUBAI
December 17-19, 2019
ame@pecb.com

To reserve your seat please contact the organizers in the emails provided above.

SPECIAL THANKS TO

PLATINUM PARTNERS



GOLD PARTNERS

glasspaper

KTMC LTD KAIZEN TRAINING & MANAGEMENT CONSULTANTS LTD

IGP Peru
INNOVACION GESTION & BUENAS PRACTICAS

WATCHCOM
A COMBITECH COMPANY

Sentinel Africa
Risk Management Consultants

KOENIG
step forward

CYNTHUS

SYSDREAM
IT SECURITY SERVICES

inlexso
INNOVATIVE LEGAL SOLUTIONS

PINK
Pink Elephant

DATAPROTECT
Security is our commitment

business as usual

excelledia®

its2
التقنية الأمنية

BEST
EXPERTS - CONSEILS

Prime
PROFESIONAL

TSTC
ICT en Security Trainingen

Easy Standart

iST

cts
COMBINED TRAINING SOLUTIONS

etfash
environmental services

aac aswar akka consultancy

ACTAGIS
Govern your IT, Security & Business

INTI.Q
SOLUTIONS

MAXPERT

AA ABILENE
ADVISORS

AJL Consults LTD.
RC:1222233

protiviti



To get more information about our trainings,
contact us at marketing@pecb.com.