

DATA PRIVACY LAWS, STANDARDS, AND REGULATIONS

WHAT YOU NEED TO KNOW



PECB Insights Magazine

delivered to your mailbox

Issue
39

PECB Insights

ISO STANDARDS AND BEYOND

JULY-AUGUST 2022

NETWORK SECURITY, ETHICAL HACKING, AND CYBERSECURITY

PROTECT YOUR ONLINE PRESENCE



LEADERSHIP THE STANDARD EXPERTISE TECHNOLOGY BUSINESS & LEISURE
WORK-LIFE BALANCE SUCCESS STORY OPINION BOOKS INNOVATION

Subscribe & find out more at

www.insights.pecb.com

In This Issue



6 The Standard

Foresight trend report: How digitalization and service excellence is a win-win

8 The Expert

The Impact of Data Governance on Cybersecurity

14 Opinion

Why is the Implementation of ISO/IEC 27701 Important for Your Organization?

20 Success Story

Exquisite Certification and Audit Limited – A Success Story

24 Innovation

The Future of User Experience – Internet of Behavior (IoB)

28 Work-Life Balance

The Lifestyle of a Data Privacy Expert

34 Insights Conference

PECB Insights Conference 2022

40 The Expert

DoS and DDoS: The Comparisons Between Denial of Service vs. Distributed Denial of Service

46 Leadership

Data Privacy Laws: GDPR vs US Data Privacy Laws

52 Books

The Importance of Data Privacy

56 Technology

How Technology Innovations are Helping in Securing Data

60 Business & Leisure

Training in the Green Heart of Europe

74 The Expert

Data Privacy Automation – What You Need to Know

78 Career

Top Five High-Paying Job Positions You Can Pursue with an ISO/IEC 27701 Certification

80 PECB University

A First-Hand Experience of Studying at PECB University

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

© PECB 2022. All rights reserved.

**“If you care
about privacy
online, you
need to actively
protect it.”**

ROGER DINGLEDINE

Computer Scientist





Foresight trend report: How digitalization and service excellence is a win-win

The possibilities of digital technologies are dazzling, but with them come challenges, not least in the realm of customer service.

[The ISO Foresight Trend Report](#) highlights global trends across multiple industries that will shape strategic decision-making for a better future. Drawing upon these insights, ISO reflects on some of the potential areas for standardization work. In a series of feature articles, we unpack some of the critical global trends with top experts in their field.

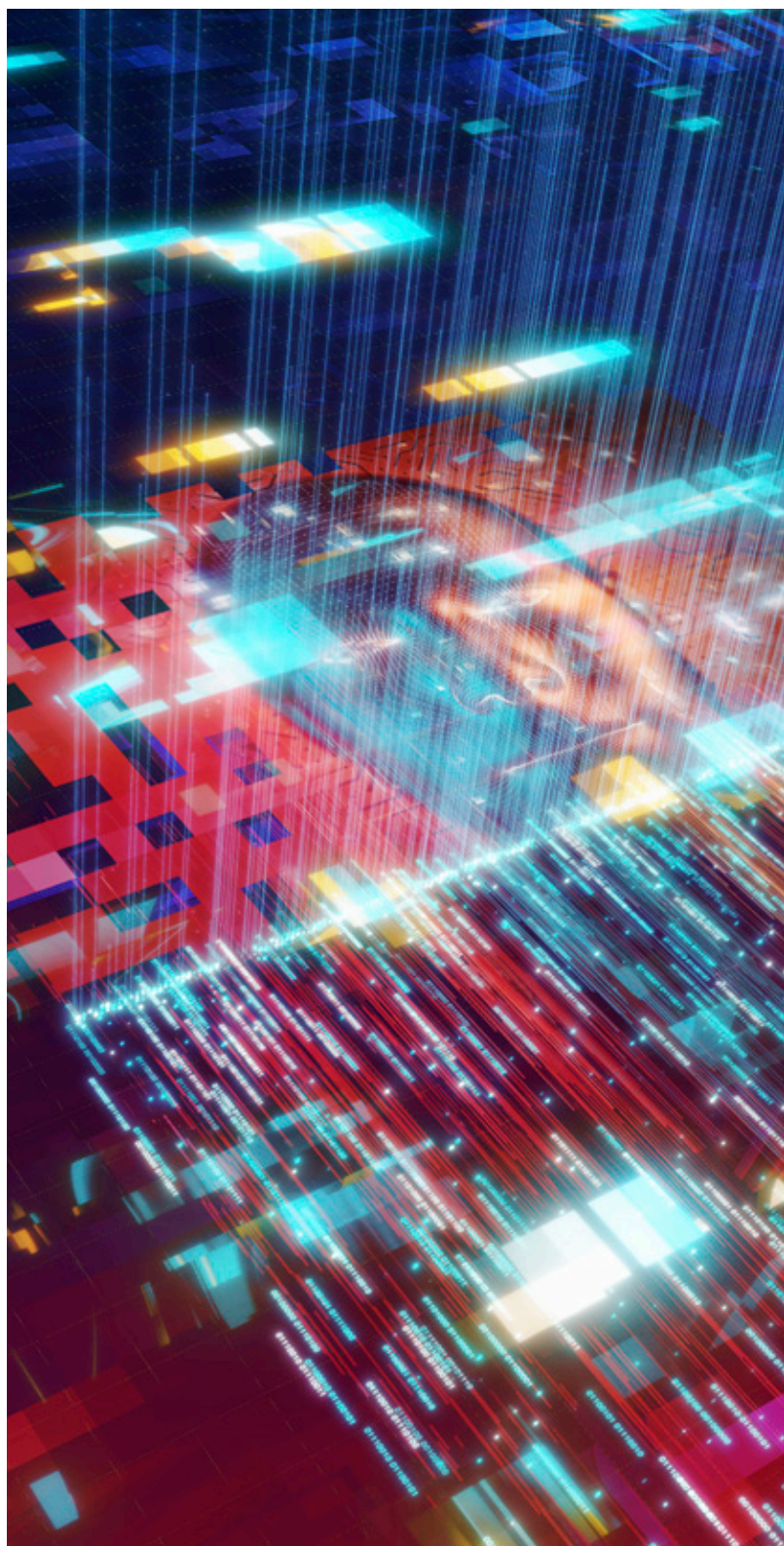
The world is more connected than ever, with new people, systems, services, and experiences just a few clicks away. Meanwhile, the shape of the Internet is changing as mobile and wireless technologies become the basic tools of communication and the number and variety of Internet-connected devices grow. By 2025, the number of devices connected to the Internet is [forecast to reach 50 billion](#).

This ever-more-connected world presents opportunities and challenges that will require forward-facing thinking to navigate. Not least with regard to the relationship between consumers and service providers. It's no secret that how well you serve customers will define your company's long-term success. In fact, excellent customer service leads to various benefits for a company, i.e. better customer loyalty, higher revenue, and lower costs. But if you have to focus on the customer and become a service-oriented organization, it's not merely enough to attain a passable grade. You have to strive for service excellence to reap its benefits.

ISO is leading the efforts in excellence in service. Experts from around the world are participating in the work of technical committee [ISO/TC 312](#) to provide an internationally agreed-upon understanding of excellence in service and models for achieving it.

The world becomes digital

The rise of the Internet is no less than revolutionary – according to estimates, the influence of the Internet over the next 15 years will [surpass the impacts of 50 years of](#)



[industrial revolution](#). It is vital to keep pace with the new battles being fought in this changing landscape.

‘You have to strive for service excellence to reap its benefits.’

With [increased connectivity](#) comes increased vulnerability to cyber-attacks: from small-scale to state-backed attacks, with implications for the security of the critical infrastructure. The Internet becoming the main source of information has made the spread of disinformation a potent new danger, forcing regulators to balance freedom of expression against the need to counter harmful content. Increasingly, those who control Internet access have enormous power – and enormous responsibility not to misuse it. According to the World Economic Forum, [at least 23 % of countries](#) censor news or block certain websites entirely.

Meanwhile, providers in this increasingly digital world – even traditional service industries such as hospitality and insurance – have a growing collection of responsibilities to their customers. All providers will be expected to invest in cybersecurity measures, have data protection policies, and consider the accessibility of their digital offerings (apps for different mobile operating systems, for example).

Next-gen connections

5G, the next generation of mobile technologies, will connect not just people but things in a vast network where massive quantities of real-time data are exchanged almost instantaneously: the Internet of Things (IoT). This is expected to bring IoT applications like driverless cars into the mainstream. 5G could contribute [up to USD 12.3 trillion to global economic output](#) over the next decade.

5G has already arrived in countries including South Korea, the US, the UK and Germany. Significant investments will be required for developing countries to keep pace – by 2025, the [share of 5G in total connections](#) is expected to reach 59% in South Korea, but just 8% in Latin America and 3% in sub-Saharan Africa. Without a change in direction, 5G and its benefits will remain out of reach for much of the world. To maintain service excellence, providers will need to bridge the divide between those consumers who have access to 5G and those who don't.

‘ISO is leading the efforts in excellence in service.’

Digitalizing services

Services are moving online, accelerated by the COVID-19 pandemic, with even habitually “in-person” industries like tourism and traditional retail industries moving to provide more digital offerings. This boosts accessibility, efficiency and affordability, but also creates new responsibilities, such as managing customer data responsibly and increasing the customer's acceptance of new digital services.

As services go digital, businesses and other organizations will face fresh challenges from shifting customer expectations, such as the relatively recent expectation for all businesses to provide a seamless and outstanding customer experience across all contact channels. Every level of the [“Service Excellence” Pyramid](#) – which lays out how organizations can improve their services to exceed customer expectations – will be reshaped by digitalization. Organizations may find themselves having to go above and beyond to provide excellent customer service, such as creating apps and using technologies like artificial intelligence, machine learning, augmented reality, virtual assistants, and blockchain.

The progression toward digital services presents fantastic opportunities for businesses in developing countries to compete internationally. This has already been identified by many governments keen to seize these opportunities – in Africa, [countries are spending an average of 1 % of GDP on digital investments](#). Kenya, for instance, is [recognized](#) for its thriving mobile banking service industry.

The shape of digitalization

With everything – from corporations to smart fridges – moving online, there is a world of things to consider to ensure that this shift is conducted safely and fairly. For instance, the recent controversy over the storage of user data by Internet companies and a need to build trust has rapidly made responsible handling of data a core service for a variety of organizations.

In the coming years, this will likely become an area ripe for standardization. The connected future is taking shape – and standards will be an important step in ensuring that it works for everyone. Those who stand to benefit are especially the customers, who will receive excellent service.

Disclaimer: PECB has obtained permission to publish the articles written by [ISO](#).

The Impact of Data Governance on Cybersecurity



BY FÁBIO ANJOS

THE EXPERT

The 21st century presents a series of transformations in the business environment and in people's lives in relation to the 20th century. The concentration of people in large urban centers, difficulties of locomotion, and social interaction, the need for agility and availability of communication, and not to say, promote physical and mental health in an environment in which the speed of interaction becomes increasingly necessary.

In the 1980s, people and businesses related in a very different way, without the presence of computers and the internet. The business needed a physical presence and direct interaction for its feasibility, that is, everything was done and carried out in a face-to-face manner.

The advent of the Internet and technological innovation have promoted an indisputable revolution in the way people consume products and services. Virtualization in consumer relationships and people's personal lives has brought much more flexibility, productivity, and ease, however, all this has a price that can sometimes be very high.

Technological evolution has narrowed the gap between those who are far away, and ironically, drove away people who are physically close, to the point of observing people from the same family gathered in the same environment without any social interaction, since they are busy with their smartphones.

The social transformation promoted by technology certainly made people's lives easier while upsetting the exposure of sensitive information and data, transforming information related to buying and consumption habits, personal data, preferences, and other intimate information into business opportunities for many companies. Not only by this massive exposure of people's lives, personal information, and that of companies, there is still the risk of criminal actions in cyberspace and an increasing need to enhance security.





The criminal activities that occurred in the physical environment gained virtual modalities with very significant impacts, often leading to fatalities due to the intimacy exposure.

Now, if there is a social transformation perceived and impacted by technology, the sharing of data, and information on the Internet, it would also be natural to imagine that social and individual protection actions could accompany the perceived change in people's lives. The protection of intellectual property on the Internet, personal data, and the sensitive data of individuals and companies, which have become the object of the desire for cybercriminals, require effective protection and legal support so that the accountability of those who commit virtual crimes, which were not previously properly typified in the traditional legal system, can be identified and punished. However, classifying actions in the cyberspace as criminal actions is not an easy task.

Many trouble-causing agents for many people do not define their actions as criminal and even fraudulent actions. Many, moreover, claim only to pursue a professional activity that depends on mining and sharing (in a remunerated way or for various benefits), and thus, are not causing direct harm to people. The data, for these agents, are only assets that have their relative value, often difficult to be measured, and despite being intangible, can represent a lot to the holder by revealing who they are, their income, their health status, beliefs, habits, sexuality, gender, culture, profession, family structure, work address and housing, gastronomic tastes, etc.. Virtual life has become a "dangerous city", full of challenges and many risks!

Many laws were contextualized and had a legal interpretation related to the social fact so that its scope could generate certain protection for those who had their data violated in some way. Laws were also created to

ensure that fundamental rights, such as privacy could be protected from criminal acts and also from unauthorized and indiscriminate sharing.

In Brazil, there is a legislation called "Civil Framework of the Internet", Law 12.965/2014, which establishes principles, guarantees, rights, and duties for the use of the Internet, as well as a specific law to ensure the proper use of data, called the General Law for the Protection of Personal Data, Law 13.709/18. In Europe, the GDPR (General Data Protection Regulation) has brought an encouragement so that privacy can be treated responsibly and respectfully for the rights of individuals.

GDPR – “Principles relating to the processing of personal data”, established that:

Personal data must be:

- a. Lawfully, fairly, and transparently treated with regard to the data subject (lawfulness, fairness, and transparency)
- b. Collected for specific, explicit, legitimate, and unprocessed purposes in a manner incompatible with those purposes; Further processing for public interest file-building purposes, for scientific or historical research purposes, or for statistical purposes, shall not, in accordance with Article 89(1), be considered incompatible with the initial purposes (limitation of purpose)
- c. Relevant and limited to what is necessary for the purposes of which they are processed (data minimization)
- d. Accurate, and if necessary, up-to-date; all reasonable steps shall be taken to ensure that inaccurate personal data, taking into account the purposes for which they are processed, are erased or rectified without delay (accuracy)

- e. Maintained in a manner that allows the identification of data subjects, for no more than necessary purposes, for which personal data is processed; personal data may be stored for longer periods to the extent that personal data is processed solely for archival purposes of public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1), subject to the implementation of appropriate technical and organizational measures required by this Regulation to safeguard the rights and freedom of the data subject (storage limitation)
- f. Processed in such a way as to ensure the proper security of personal data, including protection against unauthorized or illegal processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures (integrity and confidentiality).

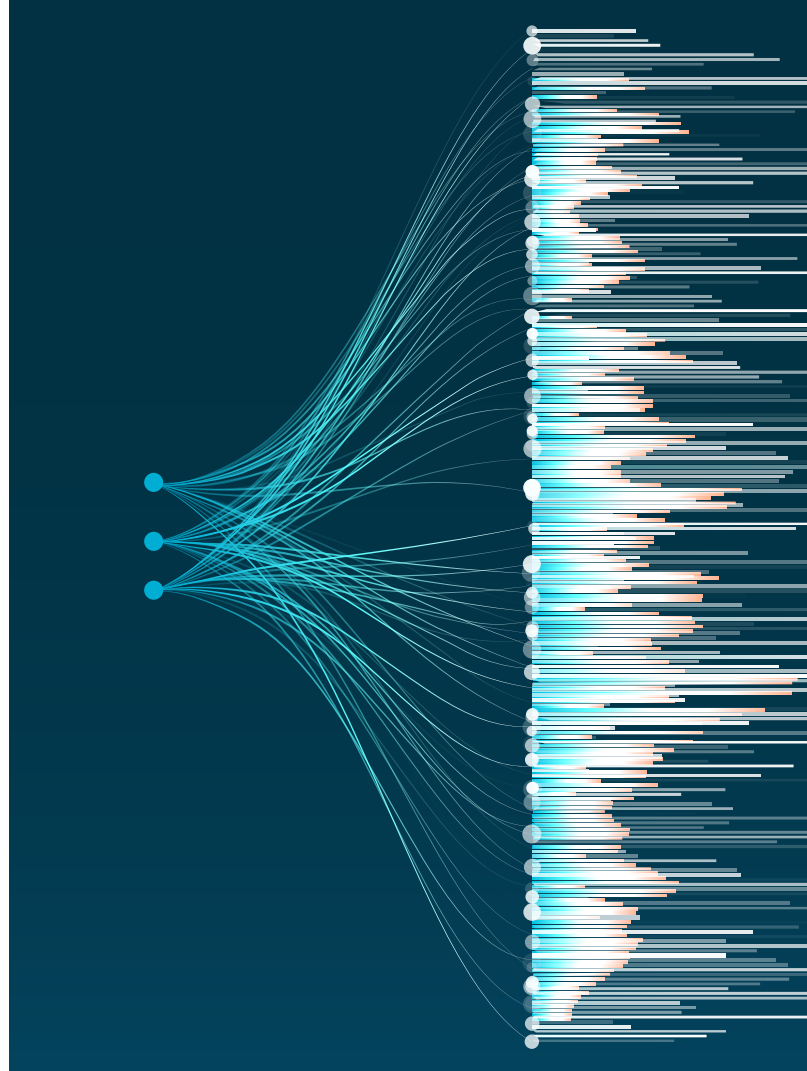
The controller must be responsible and be able to demonstrate compliance with the first paragraph (accountability).

Notwithstanding the scope, applicability, and relevance of laws and regulations of each country, it is essential to establish a culture related to responsible personal conduct in relation to your data and the data of others, whether individuals or legal entities, personal or professional data, and why not, whether sensitive or not. For British mathematician Clive Humby: "Data is the new oil" and The Economist in a recent publication defended the premise that: "The world's most valuable resource is no longer oil, but data."

If data is a very valuable asset, it can be assumed that it would be correct to claim, have the right of possession, and use properly protected data, and therefore, their owners should keep them safe with the same criterion that they hold other valuable assets safe, such as money, jewelry, or assets, should not they?

In practice, however, people neglect their data and do not align their virtual behavior with the same security behavior they adopt with other valuable assets. The pandemic has increased people's access and time in virtual environments and has certainly also increased the exposure of their sensitive data.

Referencing the behavior of individuals when trying to identify the impacts of data governance on cybersecurity may seem a misfit or even an inappropriate approach, however, the lack of governance on the part of people, especially in relation to their data, ends up unquestionably exposing people's fundamental right to cyber-attacks of



various natures and forms, of equally diverse and significant impact. Data governance is the factor in exposing assets to cybercrime.

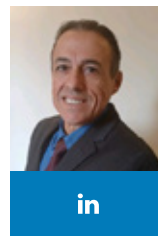
In the business environment, data governance according to [Santos](#) (Uma proposal for Data Governance based on a method of enterprise architecture development), emerges as a multidisciplinary action that aims to treat data as an active and tangible resource in the organization. This includes policies, standardizations, processes, and technology, essential elements in data administration.

Complementing the author's definition, even in a false claim, I dare say that good data governance has a direct impact on the perception of cybersecurity. It is not enough, therefore, to implement governance without minimum criteria that can relate governance actions as practices that strengthen cybersecurity in a way that can protect people and organizations. Good data governance requires a close look at human behavior, whether in the role of the user of organizational applications and software, or in the social interaction performed in personal and corporate social networks.

Good governance should be structured in detailed analysis of the relevant risks, in the assessment of the fact and

an organization. Other ISO standards can serve as support to structure and improve good governance in companies.

In addition, personal and professional development is also an ally for improving data governance and the organization itself as a whole, helping to increase cybersecurity, which is increasingly impactful in people's lives. PECB – Professional Evaluation and Certification Board, has a wide range of trainings that allow a professional to acquire and develop skills related to Data Governance, Information Security, and Cybersecurity, among others. One of the best ways to promote improvement in people's lives and markets is to acquire and disseminate relevant knowledge on topics that are crucial to people.



Fábio Anjos

Executive Director – Behaviour Brasil

Prof. Fábio Anjos is an ANPPD member, specialist in Information Security, Certified as a Lead Auditor and Lead Implementer for: ISO 9001, ISO 22301, ISO 37001, ISO 37301, ISO/IEC 27001, ISO/IEC 27701, and ISO 22301, Certified Outsourcing Manager for PECB, Risk Manager ISO/IEC 27005 and ISO 31000, Asset Manager ISO 55001, specialist Compliance Manager, specialist in Risk Management, specialist in Resources Management (FGV), specialist intermediation in financial investments (FGV), Business Administrator, pension specialist, specialist of Public Welfare and a private degree in entrepreneurship, Excellence in Customer Service (UBB group); ESG, Security Information and Data Privacy Officer.

Postgraduate Education in Higher Education, lecturer, and expert in the areas of corporate finance, corporate behavioral training for sales teams, teams business, administration, and finance, with extensive experience in corporate sales both wholesale and retail. Awarded excellence in customer relations in the financial market and excellence in the management of people and processes.

Fábio currently holds the position of Executive Financial Market, with extensive knowledge in corporate training, consulting, and development of personalized proposals in the implementation and the audit of various ISO standards. Certified PECB Trainer for Management Systems Training Courses of ISO 9001 to ISO 55001. With experience in mapping, process analysis, and production projects, identifying and resolving any "bottlenecks" in the business chain.

University professor, Master Certification (PECB) in ISO/IEC 27001 and ISO/IEC 22301 through Behaviour Brasil. Over 35 years of experience related to business processes, administration, and business management.

Contact: fabio.anjos@behaviourbrasil.com.br and www.behaviorubrasil.com.br

social phenomenon, in the culture and habits of people, and in the dissemination of good practices (inside and outside) of companies. Guides, standards, and frameworks should be widely disseminated, discussed, interpreted, and applied in companies and people should be developed (both professionally and personally) to take practices that have produced traceable and measurable results and that enable them to increase cybersecurity and protect information and data assets. Structured, timely, pertinent data governance aligned with social reality and due temporality are important allies to promote not only cybersecurity but also promote responsible and transparent interaction between the physical and virtual world.

ISO/IEC 27032 – Information Technology – Security Techniques – Cybersecurity Guidelines is one of the available resources that can help an organization implement a set of best practices capable of increasing cybersecurity. Its use, allied with standards such as ISO/IEC 27001 – Information Technology – Security Techniques – Information Security Management System, and ISO/IEC 27701 – Security Techniques – Extension of ABNT NBR ISO/IEC 27001, and ABNT NBR ISO/IEC 27002 for information privacy management – Requirements and guidelines, promote a series of widely used practices with measured and recognized results structure good data governance in

International Day for Disaster Risk Reduction

Governance has much to do with the effective and efficient way of handling natural disasters. It is clear that to reduce risk factors we need a clear vision, plan, and a completely empowered governance that takes action in accordance with scientific evidence for the greater good of the public. We all have a role to play and to help become better equipped to withstand natural disasters. The UN acknowledges that education, training, and information exchange are good ways to do so.

You can gain a clear understanding or enhance further in a career in Disaster Recovery by getting certified through our Disaster Recovery training courses.

FIND OUT MORE





Why is the Implementation of ISO/IEC 27701 Important for Your Organization?



BY MOSTAFA ALSHAMY

Looking around us we will find all surrounding people, whether they are elderly individuals, adults, teenagers, or even children, holding at least one smart device addictively and forgetting their actual physical place and people around as if they are living in another virtual world where they can do what they like when they like. The addiction increases whenever they are younger and their use and demand for content is widely different; covering memories, news, chatting, business, games, videos, audio, among so many others, but this does not matter as all of them are sharing their personal data without even knowing that.

In business, the situation is totally different as corporates have two different types of personal data, namely customer's data and employees' and partners' data. All the time these corporates are trying to serve their customers better to achieve their organizational objectives and gain their customers' loyalty. To do so, they are trying hard all the time to collect, analyze, process, and store their customer's data in a manner that in many cases does not respect these customers' privacy rights or new privacy regulations.

In some cases, some corporates make millions and billions of dollars per year by processing their customers' data in a specific manner to know how they think and behave, and this gives a great malicious advantage to corporates over customers. In many cases, we cannot call these individuals customers as they are using the corporate's applications and services for free, and therefore, the term "data subject" is replacing the "customer" to represent all types of relationships between corporates and individuals even if it is a commercial one.

Having the two types of personal data usage, which are individual and business, and taking into our consideration



the frequent news about privacy breaches and their impact on data subjects and corporates, we can understand why we have more and more regional and national privacy regulations with huge penalties.

What is Personal Data?

Personal data is any piece of information that can directly or may indirectly lead to recognizing a human being, including name, date of birth, address, phone number, and email address. Also, physical characteristics like weight, length, the color of skin or eyes, sex, blood type,

and reaching to biometric and genetic features. It can be financial like salary, loans, amounts of installments, sources of income and types, and prioritized expenses. One of the most common types of personal data collected and analyzed lately is relationships and data shared during personal and business communications. All these types of personal information among many others are collected and analyzed without the knowledge or consent of their owners to be used for secret purposes which are in many cases malicious and illegal.

What is Privacy and Why it is Important?

Privacy is the right of everyone to keep his own personal data protected from exposure by anyone else to be used for any given purpose. Due to the lately increasing personal data breaches and how many businesses are abusing the personal data of millions and billions of data subjects we started to hear about regional and global regulations like the GDPR and many national ones. The United Nations Conference on Trade and Development (UNCTAD) announces that 71% of countries have data protection and privacy legislation, 9% have draft legislation, 15% do not have legislation, and 5% of countries provided no data on legislation.

These laws and regulations were created to protect personal data from being collected, analyzed, processed, and kept without having clear and proper consent from their data subjects. There are some interference types if personal data were put in the wrong hands like decisional interference by affecting the individual decision-making process and the resulting decisions, self-representation by representing an individual in a specific manner by using their provided and shared personal information and intrusion by disturbing individual solitude or tranquility. We can find many data subject suffering from different types of cyberbullying and harassment due to many techniques including social engineering which is so much more successful in many cases.

At the same time, corporates are considered victims just like individuals when the personal data of their data subjects which can be the personal of their customers, employees, and even business partners or suppliers, are breached in any manner. This breach will lead to paying ransom to the attackers, paying penalties to regulators, and paying compensation to customers in addition to losing them and the corporate's image in the market.



To know how much privacy is important just think about the impact of breaching it from a personal or business perspective. Individuals can have huge impacts including, and not limited to, losing the respect of others in their communities, source of income, professional credibility, ability to make decisions, participation in elections, and potentially reaching to personal health and safety. For corporates the impact is much bigger based on the nature of personal data they have and process and where their business processes are located and under which applicable laws and regulations. Therefore, we can find many corporates are investing huge amounts of money in protecting the personal data they store.

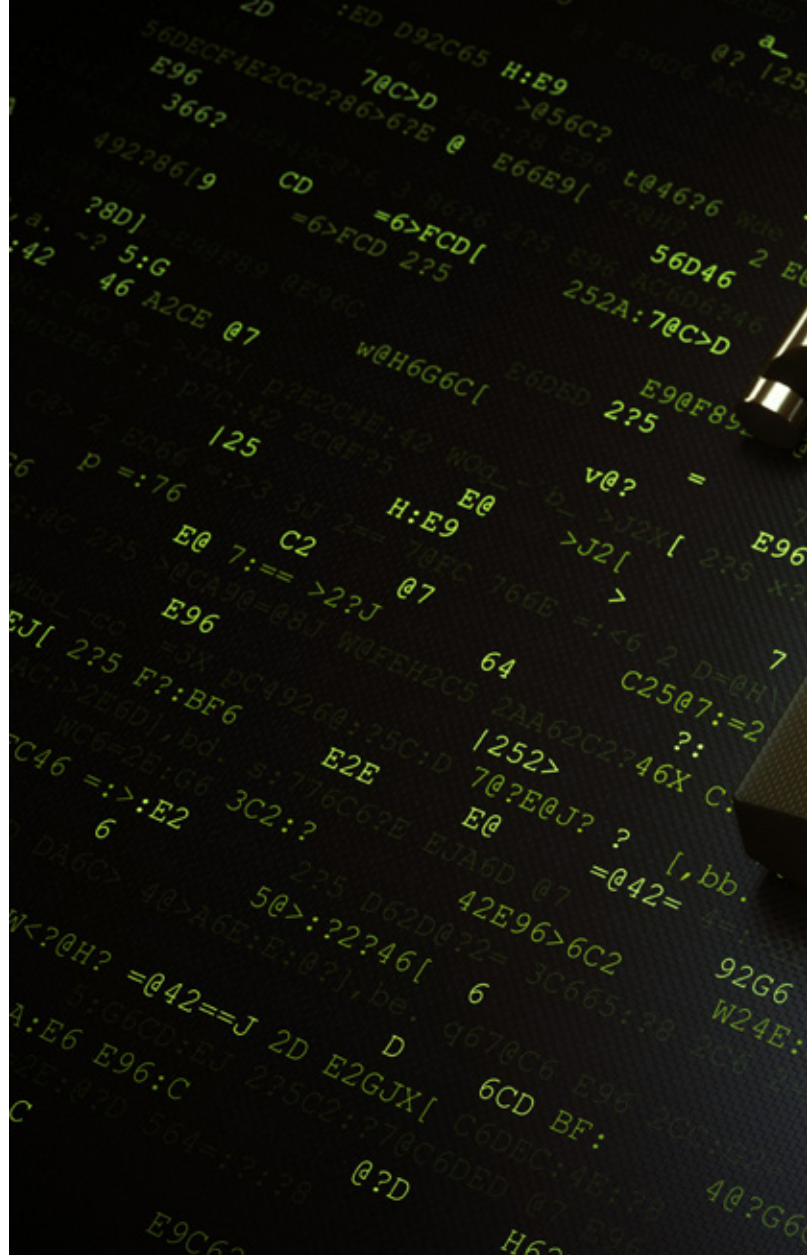
Privacy for Individuals and Corporates

I think it is clear that nowadays personal data is collected and shared in clear and unclear manners and its impact can easily reach individuals and corporates. This necessitates the need for proper awareness for different types of audiences. Who is responsible for planning and conducting awareness is totally different, as in some cases it can be governments for citizens and residents or tourists, corporate HR and Cybersecurity departments for employees, suppliers, and customers or individuals increasing their own awareness and changing their daily habits and data behavior.

There are many national awareness programs as Privacy Week in New Zealand, Privacy Awareness Week in Australia, Data Privacy Week in Canada, and Privacy, Safety, Security, and Trust Online in Philippines, among many others. Three years ago, Dubai Police has reproduced and published the famous “It wasn’t me” song with a lot of awareness lessons to all citizens and residents about how to save and not share their banking information with the support of many local banks. Two years later Egypt has done the same and many other countries all over the world are thinking about having similar public initiatives of awareness campaigns to increase the privacy awareness of their people.

Are Privacy Regulations and Standards New?

If we consider GDPR among other lately released privacy laws and regulations and ISO/IEC 27701:2019 are the first of their kind, we are wrong as there were some earlier laws and regulations like Data Protection Directive in EU since 1995 and ISO/IEC 29100:2011 Information Technology – Security Techniques – Privacy Framework among others. Privacy laws, regulations, and standards evolve over time and now we witness a great level of using and



sharing personal data geared by the immerse social media applications and platforms which collect and process the personal data of billions of users all over the world. Can you imagine that more than 140 years ago and exactly in 1890 the two attorneys Samuel Warren and Louis Brandeis wrote the article “The Right to Privacy” and published it in the Harvard Law Review?

Privacy Costs and Impacts

Whenever the costs of implementing a Privacy Information Management System (PIMS) in a corporate are calculated, the impacts of breaches, attacks, and penalties must be calculated first. Nowadays we hear about some penalties reaching hundreds of USD millions and in some cases, corporates cannot survive after some privacy cases. Impacts are also evaluated based on the type of data affected and their criticality to their respective data subjects and their interests.



GDPR for example imposes huge fines if personal data is breached or misused by the organization reaching 10 million Euros or 2% of the organization's annual global turnover and up to 20 million Euros or 4% of the organization's annual global turnover whichever is greater. In other words, this can mean hundreds of millions for some of the tech giants we have today with their turnover exceeding billions of Dollars or Euros. The Saudi Personal Data Protection Law (PDPL) imposes fines reaches to 5 million Saudi Rials that can be duplicated and 2 years of imprisonment. These two examples are a sample of so many new privacy regulations that start to enforce organizations to protect data subjects' rights of privacy and remove or reduce the potential impact of breaches or misuse.

If the top management of organizations considers the diverse impact on their organizations and their data subjects due to any negligence, I am sure they will invest in implementing powerful and effective PIMS.

Some other organizations will do it as an advantage and not only for compliance purposes, which I respect more. In one of my academic research articles, I am proposing an Enterprise Governance of IT "EGIT" Maturity Model "MM" which measures four main pillars, which are; Service Management, Information Security Management, Business Continuity Management, and Compliance Management which is a very important pillar lately due to its great impact on organizations.

ISO/IEC 27701 Benefits

ISO/IEC 27701 was released in 2019 to cover the international needs for privacy management systems and after the release of new laws and regulations and the update of others. It is based on ISO/IEC 27001:2013 and considers the existence of an Information Security Management System (ISMS) certification as a prerequisite. There are many benefits from implementing and certifying a



Each journey has specific stakeholders and needs resources and covers a specific part of the PIMS lifecycle.

The first journey is about identifying the organization's context by understanding whether the organization is a controller, processor, or both. A controller is the one who decides why data is collected and how it will be used and how it will be processed as well. While the processor is the one who processes data on daily basis. In the past organizations were playing both roles but lately, and with the increase of outsourcing and cloud services, many organizations are considered controllers, and one or more of their partners or suppliers are considered their processors. In this case, the controller is still responsible for privacy compliance governance and the processor is responsible for privacy compliance too. The best-case scenario is to have the organization playing both roles, but this is very rare nowadays. In this journey, understanding the types of personal data collected, processed, and stored is very important, in addition to the types and nationalities of data subjects which is very critical to understand applicable laws and regulations and their respective requirements and implications.

The second journey will be the implementation of PIMS which covers the organization's and its data subjects' needs by hiring one Data Protection Officer (DPO) and one or more privacy technologists if the organization does not have any to start analyzing the data lifecycle stages and support in conducting Privacy Impact Analysis (PIAs) and Data Protection Impact Analysis (DPIAs) to understand the impacts of breaching processing and storing data subjects' personal data. After analyzing the current situation and applicable laws and regulations, a project with clear roles and responsibilities will be initiated for developing PIMS which will be specific to each organization based on its specific context. During this project, there will be many components developed like the Privacy Policy which contains the top management's intention regarding privacy and the Privacy Statement which will be presented to data subjects when needed. Building systems that are less susceptible to attacks will be a core principle in the organization by following what is called Privacy by Design (PbD) and its principles and requirements.

All the organization's internal processes and systems will be updated to collect, process, and store fewer data and an external relationship with partners or suppliers will be reshaped accordingly. Clear measurements will also be embedded into all respective processes and systems with powerful technical training for technical engineers and frequent awareness to all other employees.

PIMS based on ISO/IEC 27701:2019 which can be realized during the implementation journey and after getting your organization certified. These benefits will differ based on the nature of your organization and whether it is a private, governmental, or NGO organization and where its data subjects are located.

The most important benefit is that ISO/IEC 27701:2019 was built taking into consideration the existing privacy laws and regulations and covers almost all their requirements and specifications which are identical in many cases. Therefore, implementing an ISO/IEC 27701:2019 PIMS means that your organization has already covered not less than its applicable local and international privacy laws and regulations by default. This will enable your organization to comply with laws and regulations in addition to other contractual requirements enforced by customers and partners or suppliers. Maybe there will be some specific requirements and specifications that still need to be implemented but they are still the bare minimum.

How to implement ISO/IEC 27701

The implementation of a PIMS based on ISO/IEC 27701:2019 is a group of journeys starting with the implementation journey, operation journey, certification journey, and continual improvement journey, and each one of them has specific characteristics.

A clear Incident Response Plan will be developed to handle any privacy incidents and to reduce its impact in addition to updating authorities and data subjects properly.

All the applicable privacy rights will be implemented and integrated with existing processes, procedures, and technical systems to cover data subject consent for collecting, processing, storing, and sharing their personal data and how to update them or even deletion. Building this PIMS based on ISO/IEC 27701 will require continual measurement and an internal audit and management review will be a must.

All these requirements will enable the organization to respect the privacy of its data subjects while protecting its assets and existence as a minimum if it does not target satisfying its customer and leading the market.

The next journey will be operating the PIMS by all respective internal employees and external partners or suppliers properly which will be a challenge at the beginning as many procedures and technologies will be updated or even replaced. Handling data subjects' requests and regulators' requirements are the main characteristic of this journey while incidents may happen every now and then.

I believe that complying with laws and regulations and respecting the privacy of data subjects is one of the basic rights of people in the whole world, now with data sharing as one of the core principles of doing business and providing services. You can choose your own journey and your roles which can be secure or victim.



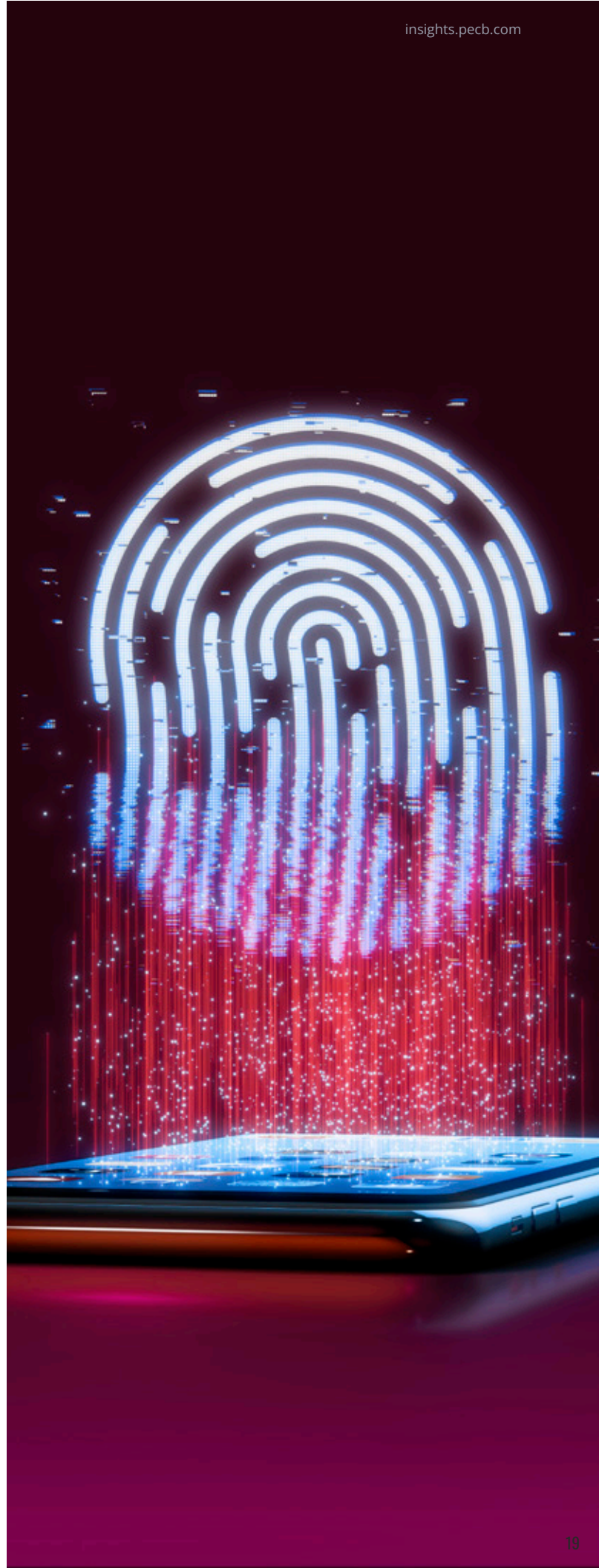
Mostafa Alshamy

Co-Founder and CEO at Ofouq Integrated Solutions

Mostafa advises the company customers on governance and management systems standards as well as trains the employees to

increase their skills and change their behavior. He is currently completing a Ph.D. degree at AAST's College of Computing and Information Technology on Organization Transformation based on Knowledge. His research interests include governance, ITSM, business quality and continuity, and information security.

Mostafa has participated and managed many ITSM and Governance projects in the MENA region, with high customer satisfaction and recognition; he has also delivered technical and management training courses to thousands of delegates.



Exquisite Certification and Audit Limited – A Success Story

Exquisite Certification and Audit Limited is a leading independent provider of certification audits and training services in Hong Kong, with special emphasis on Information Security, Privacy and Data Protection. It serves a broad range of industries, including financial sectors, IT, Data Centers, Digital Printing and Educations, to name a few. In 2020, Exquisite was accredited by the International Accreditation Service (IAS), which assures confidence in the audits of the certification body by evaluating its technical competence and quality.

In 2021, Exquisite has become one of the active suppliers of OGCIO – a governmental bureau that provides IT services and support within the government to help sustain Hong Kong's position as Asia's leading digital city.

Exquisite is an authorized training partner of PECB in Hong Kong, and the trainers are all approved and recognized by PECB. Below are the PECB Training Courses offered by Exquisite:

- › ISO 9001 Lead Auditor
- › ISO/IEC 20000 Lead Auditor
- › ISO/IEC 27001 Lead Implementer
- › ISO/IEC 27005 Lead Risk Manager
- › ISO/IEC 38500 IT Corporate Governance Manager

Trainers are the most important asset for Exquisite. They pass knowledge to others so that people could make good use of what they learned and then build upon it. Aidan Chung Tin Cheuk and Terry Lau Wai Leung, the two notable trainers at Exquisite who have obtained PECB certifications to be a trainer, are happy to share with us their “unique key to success” in their training aspects.

Aidan Chung Tin Cheuk joined Exquisite in 2020 shortly after it was established. Prior to starting his career at Exquisite, he graduated from the Hong Kong University of Science and Technology and worked as an internal auditor for a Data Center in Hong Kong. He was responsible for implementing Telecommunications Infrastructure,



ISO/IEC 20000, and ISO/IEC 27001 management systems for his company. In this role, Aidan developed excellent auditor skills which have enabled him to excel in his career in the regulatory and compliance field.

Aidan first joined Exquisite as an auditor. Within two years, Aidan was qualified to be a PECB trainer, and along with it, gained further responsibilities. Having held two internal

positions at Exquisite, Aidan's career has been varied and interesting. Each role has enriched Aidan with challenges and the company has supported his professional development by funding different qualifications to complement his work. Aidan has completed PECB certified courses, such as ISO 9001 Lead Auditor, ISO/IEC 20000 Lead Auditor, ISO/IEC 27001 Lead Auditor, and ISO/IEC 27002 Lead Manager.





Aidan Chung

Aidan has conducted over 30 classes so far and he enjoys what he is currently occupied with. “I enjoy being a trainer at Exquisite – Every day I accept a new set of challenges and I feel like I am able to help the working people by enriching their knowledge. I achieved success through training. I train myself as much as I train people,” – Aidan said. As for what the future holds, he plans to obtain some Cloud-related certifications, such as Certificate of Cloud Security Knowledge (CCSK) and Certified Information Systems Security Professional (CISSP), as he firmly believes that Cloud Computing will be in high demand in the IT industries.

Aidan enjoys the diversity of his job which presents him with new challenges every day. His role allows him to help people enrich their professional careers through professional qualifications and knowledge. His story exemplifies the core values of Exquisite, as well as the willingness to learn.

Terry Lau Wai Leung is another PECB Certified Trainer. He is also the training manager at Exquisite. Before starting at Exquisite, he worked as a senior auditor in a globally recognized certification body for over ten years, taking care of numerous projects and audits. He developed an eye for detail, excellent audit skills, problem-solving skills, and demonstrated a commitment to hard work.

Terry always has a strong desire to learn. Having graduated from The Chinese University of Hong Kong with a master’s degree, Terry knew very well the importance of self-improvement. He has obtained more than 14 qualifications from formal training and development programs to certifications, such as; PECB ISO 9001 Certified Lead Auditor, ISO 14001, ISO 45001, and ISO/IEC 27001. These qualifications made him perfect for the role of a trainer and soon he excelled on his career path at Exquisite.

As a training manager, Terry now has the additional responsibilities of delivering public training courses, as well as taking care of auditing projects. “Although Exquisite started not long ago, it has been experiencing rapid growth which provides employees with countless opportunities when it comes to learning, development, and gaining invaluable experiences. Throughout the years I have executed numerous projects and delivered over 100 classes. What strikes me the most during my work is getting a chance to work with good teammates and being able to meet professionals from different industries, and the rewards always come back as much as I contribute. This helps to keep me motivated to a better version of myself,” – Terry said.



Terry Lau

When asked about the key to making a training business successful, he said: “I don’t really have a key for it, but I believe that success is not a destination. It is a result of preparation, hard work, and experiences of failure. That’s what I have been working hard on for the past 10 years, and I’m still working hard on it. It’s like a never-ending journey but I’m starting to sip a little bit of the sweet taste of success. I guess it’s all about the satisfaction after you make the best of everything.”

Future Plans of Exquisite

Exquisite is currently targeting potential clients in Hong Kong, and targeting marketing towards the international marketplace is the next plan, “We hope to serve clients, not just in Hong Kong, but also other regions. It’s not easy, as we need to have a solid understanding of whom we’re targeting and how the people will engage with our content, but we will start it right away and see how it develops further,” – Terry said.

In 2022, Exquisite launched its e-learning platform, meant to deliver training courses with remote learning. When in-person learning is reduced, online training becomes a safe and convenient alternative for busy professionals – who are eager to refresh their knowledge. The platform hosts online courses in English and Chinese and can be adjusted to individual schedules without the risk of losing progress.

Exquisite shares common values with PECB, in that it is committed to upholding the highest professional standards and is proud to be a trusted partner of this internationally recognized organization. Exquisite continues doing its best to offer clients professional training services that can take their business performance to the next level, which is more important than ever in these challenging times. Exquisite also aims to gather representatives from different sectors to become a place where the working people can get support, meet like-minded professionals, and share experiences.

Prepared by Mia Wong, Business Development Manager, Exquisite Certification and Audit Limited.



The Future of User Experience – Internet of Behavior (IoB)



BY SOLOMON UGAH

The great advances made in the area of information technology over the past few decades have reached a perfect confluence. As the dawn of the information age came up, humans were able to deploy IT solutions to build better communication tools and to make these tools even smarter. Technology, as applied to tooling brought things like CRM, ERM, and automation chain solutions. It also changed how humans interacted with each other with the rise of social media platforms. As our tools got more intelligent, the era of the Internet of things (IoT) was born. The sheer ubiquity and the pervasive nature of smart tools and devices around the world and in our lives have yielded a vast trove of information about ourselves in a way that was not previously possible. Our behavior, interactions, and mental posture are usually expressed in how we interact with the material world via tools and systems.

These smart tools guarantee that human behavior can now be tracked individually and collectively at a volume and scale that was not previously possible. Advances in Big Data provide the means to collate, curate, and correlate data to reveal patterns and dynamics that were previously unknown to observers.

In 2020 [Gartner](#) listed the Internet of Behaviors as the number one item in its strategic technology trends for 2021. This shows that IoB will be a game-changer in the years to come.

[Forbes](#) magazine, in 2021, declared that IoB was the next frontier for smart technology and that it would enhance the human experience in many spheres of life.

The field of psychology has studied human behavior extensively and the knowledge gleaned has been used to shape policy, commerce, business, marketing, etc. Often individuals would enroll to be part of a small psychological study and small studies are conducted with small data sets. The explosion of human usage and human behavioral data presents an unprecedented opportunity for researchers



to scientifically observe humans in specific situations and times. They can test psychological hypotheses, discover previously unknown social dynamics, and predict trends.

IoB lies at the intersection of psychology, Internet of Things (IoT), and Big Data Analytics. It is able to yield intel not only on how humans behave but the likely motivation behind this behavior. It unlocks social and subconscious information that even the data subject may not be aware of.

The behavior of humans has a real impact on businesses, government, and academia. This explains the painstaking effort that has gone into unlocking the dynamic web of interconnected factors, subtle catalysts, hidden triggers, and remote causes that influence us. Even more important to researchers are the conditions that indicate or predict trends before they are ever obvious. The volume of data that needs to be computed and correlated is something that has previously been difficult to gather and sustain. The psychological motivation for IoB has always been present but the tolls to achieve it were lacking. While the problem of data sources has now been solved by IoT, the problem of data analysis has been resolved by pattern-detecting artificial intelligence and big data manipulation techniques.

An [article](#) by Science Direct envisions IoB as the topmost end of a pyramid built on data analytics and IoT.

Complex human interactions are difficult to quantify at scale and macro-trends are often detected very late in their development. At that point, it is often too late to make changes to capture the upside and avoid the pitfalls. Many large organizations that went bankrupt could have benefitted from early warning systems that signaled changes in the behavior of the market. One can only imagine that many corporate interests are watching the emergence of IoB eagerly.

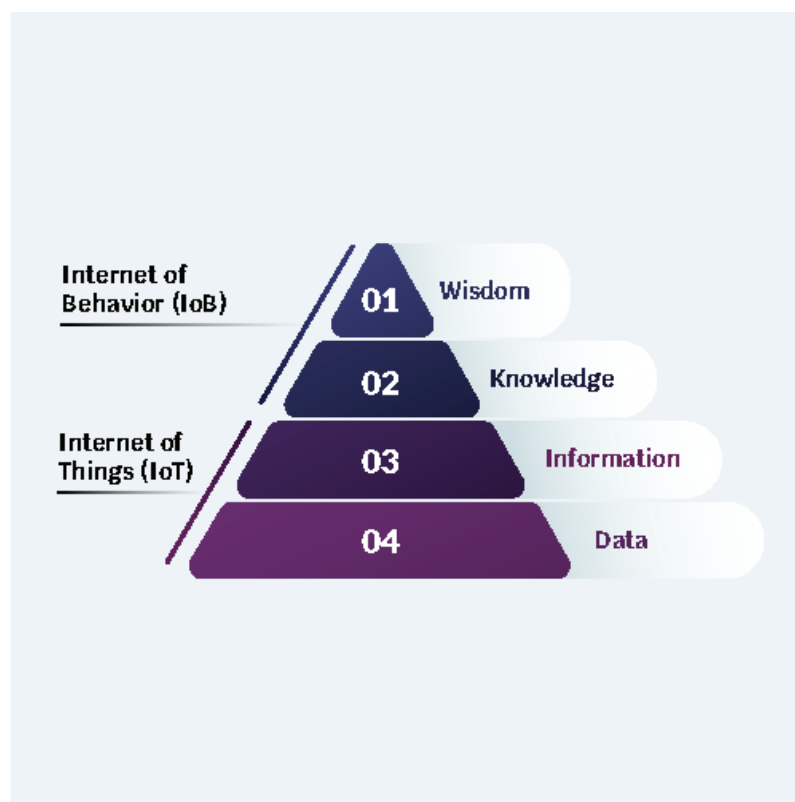
Benefits of IoB

In determining the benefits of IoB, it is important to evaluate the benefits carefully to ensure that the benefit to one party is not exploitative to another party.

Customer Service

One area where the benefits of many parties would coincide is the delivery of highly delightful and proactive customer service. The ability to analyze past data or a current data-stream to anticipate user behavior is a powerful tool for service providers to use in order to provide

customized services and tailored experiences to delight their customers. It can be deployed to provide Just-in-Time service that reduces wasted materials, effort, and time. The customer ends up with the right product they need and the service provider retains the customer's loyalty. With this benefit comes a concern. While humans enjoy customized service, it may become unnerving to know that a corporate interest knows so much about us that they can predict our lives. It also becomes very interesting when organizations compete for the same customer.



In a bid to out-perform each other, they promise even more customized service and it feels like an invasion of the privacy of the customer.

Societal Improvement

Societies change due to various factors. It could be one cohort coming of age, reaching critical mass, or change arising from a major economic shift. Public officer holders are charged with advancing the security and well-being of their jurisdiction. This often involves making policy and fiscal decisions that affect the lives of citizens over an extended period of time. These officials need insight into complex human behavior on a large scale. This is information that ensures that social strategy remains relevant for the present and the future. IoB can provide statistical models that forecast the likely effectiveness of a proposal and the resultant dynamics it creates. With this, public leaders would be guarded against solving a \$10,000

problem that creates a \$10,000,000 problem in 2 years' time. The analysis and data that IoB provides could also provide early warning signals that indicate where a social policy is causing unintended stress in another aspect of society. IoB could be the tool that helps proactively address the issues of homelessness, addiction management, carbon footprint per user, crime and illegal behavior, and reduce public resource wastage.

One obvious problem with this use case is that the citizens may feel that such precise data could be targeting a specific segment, class of society, or intruding upon their expectations of privacy.

Product Development

Product design has come a long way from the clunky and oddly-shaped designs of the early industrial age. Now designers of everything, from user interfaces to fighter jets, understand and appreciate the need to "design for humans". The human-centered design succeeds when designers are keenly aware, not only of the use case but also of the user characteristics. By deploying IoB, they can learn how people use these eproducts and evolve ways to guide better usage or discover new ways to use the product or service.

Sometimes, people do not use a product in the way the producer imagined, or people adapt the usage in ways

that could not have been foreseen. IoB would be a great feedback mechanism for producers and this leads to more life-enriching solutions.

Ethical Concerns

As with all tools and techniques that humans develop, IoB can be applied in a benevolent or malevolent manner. This raises the ethical question of the allowable boundaries of IoB. There are many pitfalls in the misapplication of this technology. Some of these are explored below.

Privacy Abuse

One concern that immediately comes to mind is that of privacy. Corporations would certainly be interested in acquiring as much data as possible about individuals, but for the most part, users are not keen on giving up so much insight into their personal lives. As news reports of data abuse and mishandling increase, one would only expect the reluctance to grow. Some other factors to consider around privacy are the issue of culture and legal jurisdiction. In one culture and jurisdiction, any use of data is permissible unless expressly forbidden, while in another, any use of data is forbidden unless expressly permitted. Another example is the difference in privacy philosophy between the US and the EU. In the EU, privacy is



protected because privacy should be protected, whether there is malicious intent or not. In the US, however, the underpinning philosophy is that privacy protection is only important to prevent malicious intent. These two philosophies color the privacy law in both jurisdictions. Human data, on the other hand, and corporate interest cross borders rapidly and are virtually impossible to lock down to one jurisdiction.

IoB related technology and investment leaders will have to navigate an increasingly complex privacy ecosystem before they can reach their full potential.

Influence Campaign

If IoB can build models to analyze user behavior, it can also be reimagined to produce models to influence user behavior. This is the most sinister aspect of IoB – the capacity to produce information and perceptions that predictively alter user behaviors and engineer social change. An individual or group of individuals could be led to behave a certain way without knowing they are being manipulated. This would find great use among corporate interests, authoritarian regimes, and shadowy organizations. The very concept of “individual choice” would be challenged because the chooser is now unsure if the action was from him or if he was manipulated.

There is certainly a huge philosophical discourse to be had around the ability of IoB to influence people. This is why this technology will be one of the hardest questions that will ever be handled by privacy practitioners and lawmakers.

What Is Next?

As organizations and industry professionals develop their strategy, they should keep this IoB technology in focus because of its ability to change service delivery models and society itself. Here are some things to consider:

Keeping Up with Opportunities

Business leaders should look for ways to ethically leverage IoB to drive customer engagement. They should actively court customer participation in the conception and design of product and service delivery. They should also see IoB as a scalpel that allows strategy to be focused and fit for purpose. Officers in strategic procurement decision positions should look out for vendors who are leading the adoption of this technology.

Keeping Up With the Risk

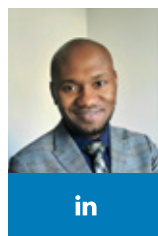
Organizations and individuals need to be aware of the evolving risks around IoB and the ways in which threat actors leverage this technology to achieve their objectives. Organizations that deploy IoB should understand the social perceptions that it creates and enhance their cyber defense to protect the PII of data subjects. Individuals should educate themselves on how the technology works and apply due diligence when using IoT, especially in facilities or environments where confidential data emanates.

Keeping Policy and Standards Up to Date

The development and revision of standards, frameworks, and policies will have to be more agile. As IoB stakeholders become even more creative in the use cases for IoB, standards have to evolve to ensure they can anticipate new developments or keep pace with current issues. There is a big risk that extant privacy and security standards will become inapplicable and unfit for adoption because they do not solve the challenges and risks that IoB technology poses.

IoB and the Future

Some may only see the dystopian effects of IoB, while others may only see the benefits to be reaped. The technology itself is neither benevolent nor malevolent, the people who use them are the ones that either use them for the benefit of humanity or otherwise. Technological advances, including IoB, will not make humans do anything malevolent they are not already capable of. It will not change us. It will only reveal us.



Solomon Ugha

Information Security and Risk Management

Solomon holds an Executive Master of Business Administration, Global Leadership from the University of Fredericton, as well as a Bachelor of Science in Applied Physics. With a wide experience in a multitude of related fields over the years, such as; Information Security and Risk Management, Cybersecurity Architecture, Privacy, Governance, and Risk and Compliance.

Solomon holds many CISO certifications on security and cybersecurity, Certified Information Privacy Manager by IAPP, Certified on Cloud Security Knowledge by CCSK, and a PECB Management Systems Auditor, ISO/IEC 27001 Lead Auditor.

The Lifestyle of a Data Privacy Expert



BY HAFIZ SHEIKH ADNAN AHMED

The past five years have witnessed unprecedented change in the realm of data privacy regulation. Since the enactment of the General Data Protection Regulation (GDPR) in Europe, jurisdictions across the globe have revisited past privacy laws and enacted new ones. While in general, the laws demonstrated a growing consensus that individuals have extensive rights over how their personal data is used, the particulars of the regulations vary widely.

As someone with a background in governance, risk, compliance, information, and cybersecurity, it is very important to keep up to date on the key trends in data privacy regulations and enforcement, best practices to ensure organizations remain compliant and avoid sanctions, and at the same time share expert perspective on the most pertinent issues in international data privacy today.

A brief introduction, My name is Hafiz Sheikh Adnan Ahmed, I am a futurist, technology, and security leader with over 17 years of record in the areas of ICT Governance, Cybersecurity and Resilience, Data Privacy and Protection, Risk Management, Corporate Excellence and Innovation, Digital Transformation, and Strategic Transformation.

Having worked with and currently working with organizations from government to semi-government and private sectors, I have seen a positive emphasis on “fair, transparent processing of personal data” over the last few years.

COVID-19 has caused a mass transfer of data to power remote work, meaning more personal data is being stored in more places than ever, and therefore, being into Data Privacy and Information Security for so many years, it is very important for me to wear multiple hats while working with these organizations at different levels of their maturity and compliance in data privacy within the organization.

Having a diverse portfolio under my belt allows me to work with multiple organizations in the capacity of a certified



trainer, data privacy advisor, internal assessor, and ISO management systems Lead Auditor.

My day starts in a very unusual way when my kids, Azaan and Aabirish, wake up early morning and start jumping on our bed and leave no choice for me but to get up from bed. Since working from home for the last few years gives me the leverage to save my time on commute and my only commute is from my bedroom to my office room on the same floor in my living space.

The moment I enter my office room, I ask a question to myself: what value am I going to add to my client's data privacy and security program, and what is new that I should expect today? And the answer is remarkably simple for me: I am not here to work to earn, but to learn and to fulfill my thirst of being the best in the field; I am here to strive for excellence and success will come to me. With this immunity booster, I start my work by checking my calendar for the day and my emails. Being an ISO geek, I strongly believe in the concept of PDCA lifecycle; Plan-Do-Check-Act. Therefore, my workday starts with the 'planning' phase, whereby I must plan my activities for the day, including both personal and professional activities. Collaborating with different clients based in distinct parts of the world (Australia, Middle East, and the USA to name a few) brings an especially important and critical factor of time management. It is particularly important for me to prioritize my day-to-day activities to achieve goals faster. This helps me to take on new opportunities and grow in a sustainable manner. My time management skills have improved to make me more self-disciplined, has improved quality of work, reduced stress, has opened new possibilities, and has enhanced my decision-making ability.

As I finish my 'planning' phase for the day in comes the Home Minister, my wife Anam, with a delicious and healthy breakfast. She exactly knows what I need and when I need; I am least bothered about my food as that department is very well-managed by her. Part of me excelling in this field is because of her as she exactly knows what food I like and at what time, and at the same handle the kids very smartly, therefore, her continuous support as my partner has played a massive role in my success.

After a small break, I start my 'execution' phase. As a data privacy, information security, and risk management SME, my daily activities revolve around a constant review of the clients' local and global data protection compliance arrangements to include updated policies and guidance, centralizing processes, and putting in place robust, time-bound remedial plans where necessary. I also need to develop and maintain relevant global internal data privacy policies and training; develop and implement a robust compliance plan; partner with all key business areas including IT Security teams, business continuity, and business development teams to ensure data privacy issues are considered at the outset of new projects, products, and initiatives.

Serving as a Certified Data Protection Officer, I also function as a liaison to the client's risk and data privacy committees in relation to information security, risk management, and data privacy issues. I must also investigate enquiries and issues relating to data privacy practices, withdrawal of consent, the right to be forgotten, and related data-subject rights. At the same time, I also need to monitor and keep an eye on the industry landscape to keep visibility on evolutions, trends, and best practices



related to data privacy. Having a strong background in Information Security, Business Continuity, Cybersecurity, and respective ISO standards as a Lead Auditor and Lead Implementer gives me an added value to ensure that systematic compliance audits are undertaken, and their findings are reported and acted upon.

Another crucial element of my day-to-day activities includes training courses, workshops, and awareness sessions around Information Security, Data Privacy, Business Continuity, Risk Management, Cloud Security, etc. Most of my afternoons, and sometimes weekends, are allocated to conduct training courses under the banner of PECB as one of their prime trainers. I have been a [PECB Certified trainer](#) for the last 9-10 years and it gives me a valuable advantage to conduct training programs and to provide trainees with the knowledge and skills to perform better in their roles or positions.

I have been fortunate enough to have conducted data privacy and privacy management training programs with more than 150 candidates from over twenty-five (25) countries since the inception of GDPR. During the training programs, we discuss topics like data subject rights, principles of data privacy, roles and responsibilities of a Certified Data Protection Officer, Risk Management, Data Privacy Impact Assessment (DPIA), Legitimate Interest

Assessment (LIA), adoption of technical and administrative controls to reduce data privacy issues and risks, incident management and the role of supervisory authorities, and correlation between GDPR and other standards and frameworks, such as ISO/IEC 27701 and ISO/IEC 29134.

After a long day's work, it is particularly important to take a backseat and get out of my office room. I spend most of my afternoons and early evenings with my family and my two kids who have their own schedule and agenda for the day to keep me busy with them in their activities. My wife, on the other hand, leaves no stone unturned to prepare some great healthy snacks that works as energy boosters to prepare me for my next phase of my evening activities, "Monitoring and Improvement."

My late evening activities involve "Monitoring, Compliance, and Improvement" for my clients based out of Middle East and the USA. Living and working in Australia gives me a time-zone difference advantage and I take maximum advantage out of it by being involved in internal and external ISO Management Systems Certification audits with different clients. Over the last couple of years, I have been able to conduct audits and assessments around GDPR and ISO/IEC 27701 – Privacy Information Management Systems, among others.

The prime focus during these audits and assessments is to examine how controllers and processors manage the collection and processing of PII (Processing Identifiable Information). Since, every organization processes PII and cooperates with other organizations regarding the processing of PII, it is particularly important to identify and understand the context of the processing of PII, as it has become a societal need, as well as the topic of dedicated legislation and/or regulation all over the world. During data privacy audits, a lot of discussions and evidence are collected around lawful basis of processing, the purposes for which the PII is processed, evidence that determines when and how consent is obtained from PII principals, understanding the need to conduct privacy impact assessment, contracts between processors and controllers covering all the confidentiality, integrity, and accountability aspects of PII, etc.

These and much other related evidence and its analysis give a reasonable assurance about the conformity and non-conformity of the privacy management system within the organization. I strongly believe that being an auditor gives a luxury and a chance to interact with new clients, understand their systems, and understand their business processes that helps me to improve my knowledge, skills, and expertise in this area. Conducting audits and training





programs over the years has improved my communication skills and has given me the confidence to build better working relationships, has increased my productivity, and to listen and convey my message to the audience in the best conceivable way.

Outside of my routine activities, I keep myself indulged in different volunteer activities, as I strongly believe that if I am blessed with knowledge, skills, and expertise, I should give back to the society in any feasible way. I do a lot of volunteer work with organizations like ISACA; I have been serving as a Chapter leader, working in different working groups as an advisor and mentor, and draft articles around the topics of data privacy, auditing guidelines, AI Governance etc. Being a certified trainer has given me the opportunity to improve my communication skills over the last few years and this has leveraged me to participate in different conferences and seminars as a public speaker and panelist.

My weekends are 100% dedicated to my family as we love to do sight-seeing, driving, and enjoying relaxing at staycations with my two little munchkins. I love exploring new resorts, new cities, driving down to CBD to sit and relax with a cup of coffee, spending time under the swimming pool to refresh my mind and soul, and gearing up with some innovative ideas. The pandemic has forced me to adapt to the changing business requirements of the market, to become more agile, and to focus on the contemporary trends and technologies like AI, Blockchain, IoT, cloud auditing, etc.

In the bigger picture, I recognize myself and want others to recognize me as someone who strives for excellence, so that when my kids grow up, they can proudly say, “Dad, we’re proud of what you’ve achieved in your career.”



in

Hafiz Sheikh Adnan Ahmed

IT Governance, Risk, and Compliance, Business Continuity, Information and Cyber Security, and Data Privacy Expert, Certified PECB Trainer

Hafiz Sheikh Adnan Ahmed’s journey started back in 2005 as a Quality Assurance Engineer and over the years, he shaped his career in the areas of information and communications technology (ICT) governance, Information and Cybersecurity, resilience, data privacy and protection, risk management, enterprise excellence and innovation, and digital and strategic transformation. He is an analytical thinker, writer, certified trainer, global mentor, and advisor with proven leadership and organizational skills in empowering high-performing technology teams. He is a certified data protection officer and won chief information security officer (CISO) of the Year awards in 2021 and 2022 by GCC Security Symposium Middle East and Cyber Sentinels Middle East, respectively.

Hafiz is a public speaker and conducts regular training, workshops, and webinars on the latest trends and technologies in the fields of digital transformation, information and cybersecurity, and data privacy. He volunteers at the global level of ISACA® in different working groups and forums. He is the Co-Founder and CIO of AZAAN Cybertech Consulting, and his role is to drive and align business strategies of the company’s esteemed clients towards Information and Cybersecurity centric and to oversee the people, processes, and technologies within the organizations to ensure they deliver outcomes that support the goals of the business. To know more about AZAAN Cybertech consulting, visit: <https://azaan.ae>. Hafiz can be contacted through email at hafiz.ahmed@azaanbiservices.com

PECB INSIGHTS 2022 CONFERENCE

November 17-18, 2022 | Brussels, Belgium

PECB is proud to host the 8th annual Insights Conference in a row, this year also marking a return to in-person conferences after a three-year period, making this an especially noteworthy event! This event will feature various new and exciting makings, where you will be able to see all the trends, and inspirations of this decade, and where you can connect with C-level professionals to discuss the latest trends and developments in the world of Information Technology, Security, and Privacy!

As part of the PECB Insights Conference, we are launching two Intensive three-day training courses as part of the Pre-Conference Training Courses in Brussels from 14-16 November 2022:

- Lead Crisis Manager Training Course
- Digital Transformation Manager Training Course

If you are a PECB Partner or Trainer, as a close part of the PECB Family, you are entitled to a free ticket to attend this event!

Contact us to receive your coupon code and do not miss this highly noteworthy occasion!

CONTACT ►

Getting to the Conference

The PECB Insights Conference will be held at the **Renaissance Brussels Hotel, Rue du Parnasse 19, 1050 Bruxelles**, Belgium.

**PECB Insights
Conference Ticket**

\$399

BOOK NOW



**PECB Insights Conference
Premium Ticket**

\$1,399

BOOK NOW



**PECB Pre-Conference
Training Course**

\$1,299

BOOK NOW



Meet us in Brussels!

REGISTER NOW ►

PECB Insights Conference 2022

NOVEMBER 17-18, 2022 | BRUSSELS, BELGIUM

PECB is proud to host the 8th annual Insights Conference in a row, this year also marking a return to in-person conferences after a three-year period, making this an especially noteworthy event! Designed to ignite and inspire, this event will feature various new and exciting makings, where you will be able to see all the trends, influences, and inspirations of this decade, and where you can connect with C-level professionals to discuss the latest trends and developments in the world of Information Technology, Security, and Privacy – with topics surrounding Information Technology, Digital Transformation, Artificial Intelligence, Blockchain Technology, and much more. This event not only includes two full days of interactive and immersive sessions but also features two Pre-Conference Training Courses. Hence, we are happy to let you know that we are launching the following, Digital Transformation Manager and Lead Crisis Manager, Training Courses as part of the Conference in Brussels from November 14-16. These sessions and courses will convene the world's most influential and brightest minds across industries. By building bridges between specialists and experts from various industries, we aim to create a community that is inclined to embrace changes and join forces toward a safer world.

It is a conference's role to bring together like-minded people from around the world to exchange ideas, generate new ideas, and inspire. Every individual benefits from attending a conference in a different way. An individual can gain insight into topics that are rarely taught in the workplace or over the internet by attending this conference. In order to meet business challenges in an innovative and creative manner, individuals benefit by being inspired by fresh ideas.

In this exclusive event, the importance of networking cannot be overstated. In addition to keeping up with new trends in their fields, conferences are an important way to connect with other professionals. The PECB Insights Conference 2022 offers the opportunity to hear from industry leaders, ask questions, and discuss the topic further than reading an article or listening to a podcast. Moreover, networking is important when you are searching for a job, and a good network can be beneficial in many ways. It can be a valuable resource to network with people from different



companies and other countries who can provide referrals, solutions, best practices, and new approaches. In addition to sharing advancements, conference attendees can also discuss problems they have encountered and strategies they developed to resolve them. Having heard from leading experts and visionaries, attendees become enlightened and encouraged to think outside the box, resulting in positive outcomes. The importance of this is especially evident when you are looking for collaborators, job ideas, or committee members in some fields. As you begin to establish yourself in your field of study, conferences are another way to get your name out there.

Another advantage of the PECB Insights Conference 2022 is that it provides a blended learning environment with numerous possibilities for people to learn and engage in a wide range of formats, with one-on-one engagements, group outings, chances for social interaction, etc., and even clarify questions you may have regarding your business. By attending, you will be able to ask questions that are not usually covered in books or blogs.

You will have the ability to gain new skills, tools, and tips or tricks. There are many different tools available, some of which show us what we have not seen yet, some of which make us faster, make us less likely to make mistakes, or provide us with some other advantage. There are plenty of these products available online, but getting a hands-on demonstration or being able to ask questions that are specific to your business struggles is invaluable. We indeed have everything at our fingertips thanks to the World Wide Web, but it can also overwhelm us with information we cannot understand or we are unable to access.

The benefits of attending the PECB Insights Conference 2022 are numerous, so we encourage you to take advantage of your opportunity!

Why attend?

- › Discover and stay current with the latest trends
- › Participate in informative talks
- › Develop professional relationships with international colleagues
- › Take advantage of valuable content
- › Expand your network
- › Meet some of the brightest minds in the world
- › Engage with the best in the business and gain insight into their practices



Program

The participants can expect to learn new insights on the latest trends, in addition to obtaining valuable information on a range of chosen topics. With a rapidly changing world, it is becoming more and more difficult to stay on top of the progress. That is why our conference program contains topics that will cover all of the latest trends and developments in the world of Information technology, with topics such as Artificial Intelligence, ePrivacy, Tokenization, GDPR, Ethical Hacking, the Internet of Things, and so much more, making it a lot easier to understand and be prepared for what's to come.

If you want to learn more about what to expect from each session, you can read more below.

[AGENDA ►](#)

Meet our speakers

You will be able to hear from visionary leaders in the Information Technology, Security, and Privacy world.

With over 50 highly esteemed panelists and four sets of two simultaneous sessions per day, in English and French, we have ensured that each participant is equally involved in topics of their interest and preference. This line-up will include speakers from world-leading organizational C-level speakers, such as the Facebook's Meta Research Scientist, the National Bank of Egypt's Cybersecurity Head, Luxembourg's Data Protection Commissioner, and many more professionals coming together to share their experiences and masteries with you! You can check out our speakers by clicking below.

[SPEAKERS ►](#)



Pre-Conference Training Courses

During this year's conference in Brussels, on the 14-16 November we will offer exclusive intensive training courses, focusing on advancing the skills and competencies of participants. These training courses will be held simultaneously, therefore, participants can attend only one of them accordingly.

• Digital Transformation Manager

Digital transformation has helped organizations across different industries in achieving long-term growth and productivity. An effective digital transformation strategy helps avoid problems during the transition and after implementation. Although digital transformation enables organizations to improve customer experience, enhance business performance, and increase their efficiency, its implementation is not that facile as it requires, among others, competent individuals, the necessary resources, including complex software and technology, changes in organizational structure, and the implementation of change management and digital transformation strategies. To address and manage these aspects effectively, organizations need a Certified Digital Transformation Officer (CDTO).

The PECB Certified Digital Transformation Officer training course provides insightful information that will help participants to gain comprehensive knowledge on digital transformation and the steps required to digitally transform a business model, including a thorough explanation and discussion of digital transformation

methodologies and approaches. In addition, participants will acquire knowledge of some of the most widely used technologies, such as artificial intelligence, machine learning, IoT, blockchain, cloud computing, and big data.

Upon the successful completion of the training course and exam, participants can apply for the "PECB Certified Digital Transformation Officer" credential.

To broaden your academic and professional skills and acquire comprehensible knowledge of emerging technologies that help meet the changing business needs and expand the digital innovation landscape, you can register for this 3-day intensive course and master the implementation of a digital transformation strategy!

Language: English

Trainer: Graeme Parker

Included: Training Materials, Examination, Certification, Lunch, and Email Support

Venue: Renaissance Brussels Hotel – Marriott, Rue du Parnasse 19, 1050 Bruxelles, Belgium

Date: November 14-16, 2022



• Lead Crisis Manager

The Lead Crisis Manager training course helps participants develop their competence to support an organization in planning, establishing, maintaining, reviewing, and continually improving its strategic crisis management capability based on the guidelines of ISO/DIS 22361 and other best practices.

The PECB Lead Crisis Manager training course helps participants develop their competence to support an organization in planning, establishing, maintaining, reviewing, and continually improving its strategic crisis management capability based on the guidelines of ISO/DIS 22361 and other best practices. It also provides information regarding the fundamental concepts and principles of crisis management and the effective establishment and implementation of a crisis management framework.

In addition to the explanation of the theoretical concepts related to crisis management, the training course provides practical examples and scenario-based quizzes that will help you reinforce your knowledge and prepare you for real-life scenarios concerning crisis management.

Upon the completion of the training course, participants can sit for the exam and apply to obtain the “PECB Certified Lead Crisis Manager” credential once they pass the exam. The credential demonstrates that the participant possesses the theoretical and practical knowledge and skills to support and lead an organization in designing and developing its crisis management capability based on ISO/DIS 22361 guidelines and best practices in this field.

To broaden your academic and professional skills and become a great crisis leader you need to be able to adapt to many different circumstances, you can register for this 3-day intensive course and master the risk management and crisis management skills!

Language: English

Trainer: Rinske Geerlings

Included: Training Materials, Examination, Certification, Lunch, and Email Support

Venue: Renaissance Brussels Hotel – Marriott, Rue du Parnasse 19, 1050 Bruxelles, Belgium

Date: November 14-16, 2022



Discover Brussels

Famous for being the political and cultural epicenter of Europe, Brussels has a lot to offer, both professionally and for leisure. Its diverse culture offers visitors a vast list of activities and experiences. With over 80 museums and an extensive history and culture, Brussels is more than just home to the European Union.

Brussels is said to be one of the most underrated cities in Europe and is home to many hidden gems for visitors to see.

Brussels is home to over 80 fascinating museums, ranging in a variety of fields. Whether you are interested in trains,

fine arts, natural sciences, or even street lights, Brussels has it all!

Join PECB in discovering these hidden beauties and making unforgettable memories.

Getting to the Conference

The PECB Insights Conference will be held at the Renaissance Brussels Hotel, Rue du Parnasse 19, 1050 Bruxelles, Belgium.

Interesting Facts

#1 Audrey Hepburn was born in Brussels on May 4th, 1929. In addition to Miss Audrey, over the years, the city has drawn in many historic figures of fame, including Victor Hugo, Karl Marx, Paul Verlaine, Alexandre Dumas, Charles Baudelaire, Auguste Rodin, and many more.

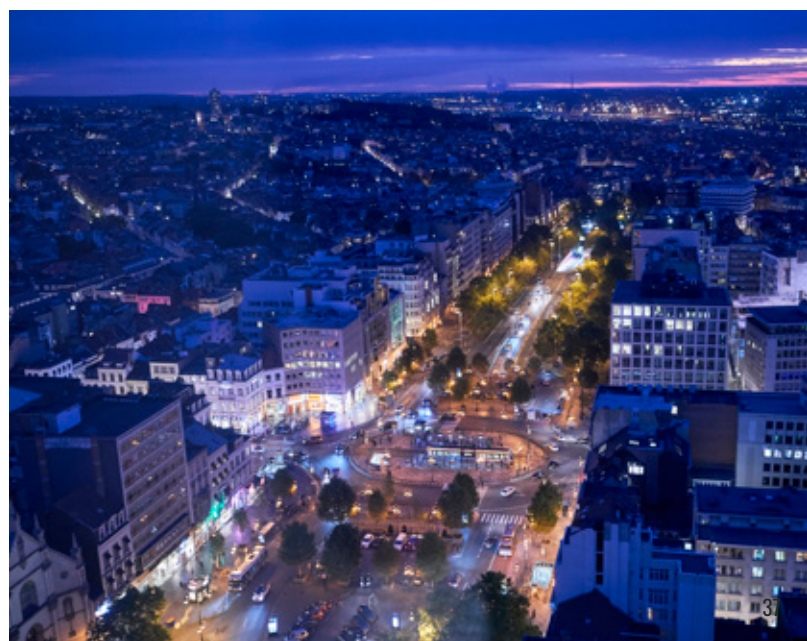
#2 The Koekelberg Basilica, or "the Basilica of the Sacred Heart" in Brussels is the fifth largest church in the world. It is also the third-largest cathedral in the country and the biggest building of the Art Deco style in the entire world.

#3 Built during the late 1900s, the Justice Palace of Brussels (Palais de Justice) remains the most significant court building in Belgium. It's also truly massive at 26,000 square meters/280,000 square feet. When it was built, it was the largest building in the world, and today it is still one of the biggest and most remarkable edifices in Europe.

Meet us in Brussels!

November 17-18, 2022

REGISTER NOW ►





Certified Management Systems Auditor (CMSA) Training Courses Available

Develop the necessary knowledge to plan and perform management system audits in compliance with the best know practices, including ISO 19011 and ISO/IEC 17021-1.

This training course will prepare you for future professional challenges, help you enhance your personal development, build networking opportunities, and achieve worldwide recognition.

Our Certified Management Systems Auditor (CMSA) training courses will be offered in both English and French during November and December.

Dates: 28-30 November

Location: Online

Trainer: Serge Barbeau

Language: French



Dates: 5-7 December

Location: Online

Trainer: Anders Carlstedt

Language: English



LEARN MORE ►

DoS and DDoS: The Comparisons Between Denial of Service vs. Distributed Denial of Service



BY GRACE LAU

Whether it is Amazon Web Services or small businesses, cloud services need to protect themselves from cyber-attacks. Two of the most common attacks are Denial of Service (DoS) and Distributed Denial of Service (DDoS).

But what are they? How do they work? And what is the difference?

In this article, we will discuss these attacks, how they work, and how you can protect your business-critical services from disaster.

What is a DoS attack?

DoS refers to a 'Denial of Service' attack.

This type of attack uses a distant computer to send many UDP and TCP packets to a specific server or network port. 'UDP' & 'TCP' are network protocols used for transferring data quickly, and 'packets' are TCP (and sometimes UDP) data units.

When this attack exceeds the system bandwidth, packets cannot get through to requests from legitimate users.

There are plenty of reasons why an attacker would try to take down the sites and servers of companies. The most frequent causes include:

- › Disgruntled current or former employees. This is another good reason to think about employee satisfaction and what is minimum wage for even your entry-level employees
- › Malicious competitors
- › Political motivations (think "hacktivism")



You might remember "LulzSec" from news headlines many years ago, who claimed to have taken down Sony's Playstation services for the "lulz".

Biggest data breaches of 2021

Records Stolen	Company or Service
5B	Cognyte (MAY)
5B	Twitch (OCTOBER)
700M	LinkedIn (JUNE)
553M	Facebook (APRIL)
400M	Bykea (JANUARY)
223M	Brazilian database (JANUARY)
214+M	Socialarks (JANUARY)
150M	Raychat (MAY)
106M	Thailand visitors (AUGUST)
100+M	Android user data leak (MAY)

Whatever the motivation, a successful DoS attack can cause significant damage to your website and business. This is why you need to be aware of the risks and take preventative measures. Let us take a look at some of the most common DoS attacks:

Buffer Overflow

The most typical DoS attack is the buffer overflow. A buffer overflow attack simply involves a cyber-attacker flooding a network's address with "traffic," rendering the network inoperable.

Ping of Death

In this kind of attack, the target machines are devices whose security is not properly set up. You might have heard of hackers targeting something as unlikely as an office's Wi-Fi-enabled printer.

It uses them to deliver fake packets from this single source that pings each and every targeted computer on the network. Because the source IP addresses are in-house, it

does not set off automated alarm bells quite as easily.

SYN Flood

SYN flood attacks start the network connection request procedure with a server, then stop the process before it is finished. An actual user cannot get legitimate traffic through because, as with all these attacks, the network becomes overloaded with high volumes of traffic.

Teardrop

In a teardrop attack, the attacker sends fragments of IP data packets that the network has to try to put back together. If it is not caught in time, the system will time out and crash trying to make sense of the missing fields in the data packet.

The danger of these attacks is that they are very simple and low-cost to carry out, but if successful, they can take a company's server down for days or weeks. If the business is a cloud service or SaaS provider, this could be devastating to them and every company that depends on them to do their own work.



What is a DDoS attack?

A DDoS (Distributed Denial of Service) attack is trickier than a DoS attack. This is because DDoS attacks several devices, making the attack much worse. Being attacked by a botnet of hundreds, maybe thousands, of hacked devices is a much trickier problem than just blocking malicious traffic to your signing systems server from one source. Types of DDoS attack include:

Ping Flood

Business phone systems use functions like call parking – this is when the system is taking more calls than there are phones to answer them. But a cloud server has no such protections built in. If the server gets too many requests at once, it will effectively shut down the system for other users. These malicious requests use "ping packets" to take a network down, which makes them comparable to UDP flood attacks. These packets will be sent by an attacker very quickly and without waiting for a response, as a legitimate actor would.

UDP Flood

A UDP (User Data Protocol) flood attacks the network with a deluge of UDP packets. The attacker's script finds a remote host and starts flooding the HTTP ports. The host keeps searching for an application that it thinks is listening at a specific port. Once the host times out or realizes there is no application, it responds with a packet advising that the destination could not be reached. This procedure exhausts a network's resources, preventing legitimate user devices from connecting.

Slowloris

The malware tool Slowloris enables an attacker to transmit insufficient HTTP requests without intending to finish them. After that, the malware transmits HTTP headers with each request in order to ramp up the attack.

This restricts the targeted network's ability to deploy resources. This will keep happening until the targeted server can no longer establish new connections.

Because the tool gets rid of the need for the bandwidth for the attacker, it is a popular tool for low-effort hackers who do not have the resources to run a big DDoS attack.

HTTP Flood

This refers to any attack that uses HTTP GET or POST requests at the application layer with the goal of attacking a particular app or web server.

Unlike other attacks, it does not require incomplete or malformed data packets, instead using well-formed HTTP requests to bombard the server with requests all at once.

Zero-day Attacks

This kind of attack takes advantage of new and undiscovered vulnerabilities. It serves as a catch-all phrase for any attack that could hit your new software or hardware as soon as you install it.

Zero-day attacks are challenging to defend against since they are "undiscovered" by definition, and there is no prior art for dealing with them.



What are the differences?

The main difference between DoS and DDoS attacks is that DDoS uses many internet connections – in contrast to DoS' single connection – to take the victim's network offline. DDoS attacks are more challenging to identify because the victim cannot accurately detect the attack's origin.

Another big difference is the amount of malicious traffic being sent in. DDoS attacks enable the attacker to flood the target network with enormous amounts of traffic, whereas DoS does not need so much.

With AI systems like GPT-3 enabling powering an instant outline generator for any content you can think of, it is no wonder we are seeing simple hacks and attacks like DDoS getting automated by armies of bots.

DDoS attacks are carried out using those botnets, or networks of hacked devices under the attacker's control.

DoS attacks, on the other hand, are often carried out via a script or a DoS tool like the famous "Low Orbit Ion Cannon".

How to Prevent DoS and DDoS Attacks

There are a number of ways to prevent DoS and DDoS attacks. These include:

Updating the site regularly

Updating your site's core codebase, front-end themes, third-party plugins, and other software reduces the chance that vulnerabilities may be exploited by hackers.

Third-party plugins in particular are a cloud cybersecurity risk if they are not properly audited by your IT team. By keeping your website updated, you also reduce the chance that it will be used as part of a botnet.

Review site logs

You may spot any suspicious activity on your site before it causes an issue by auditing server event logs. You can see issues like HTTP error codes that could be brought on by unidentified DoS attacks. Logs will also allow you to trace any cyber-attack or attempted cyber-attack back to its precise origin.

Get the whole IT team on an [enterprise communication platform](#) conference call dial-in to go over the logs and audit the logs whenever something looks out of place.

Tighten up your user authentication

Part of any engaging webinar is making sure the right people get in. When Zoom exploded in popularity there was a wave of "Zoom bombing" where strangers would appear in meetings, calls, and classes because the hosts had not set permissions properly.

If online events need that level of security, why do companies invite cyber-attacks with slack user permissions? Strong passwords which are changed regularly, and accounts protected by two-factor authentication should be the minimum standard for cybersecurity at this point in time.

Tightening up your user authentication measures is one of the easiest ways to protect yourself from DoS attacks.



Invest in anti-DoS technology

Invest in services that assist in identifying such assaults by examining network traffic, such as anti-DDoS and anti-DoS attack services.

For example, you could automatically implement "black-hole routing" in which traffic is redirected to a null route.

This diverts the DDoS traffic to an endpoint where nothing else happens to it. Because the data is not processed, your servers are safe even though the hacker's script is still firing. This failed attack, recorded in your event logs, will let you gather data like IP addresses to block them in the future.

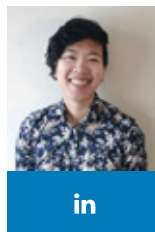
Come up with a strategy

Be proactive with a thorough DoS response strategy. When you are running a service with customers who depend on you, you need a plan for incidents like attacks or other outages. A dedicated team must be assigned to make sure every device on the company network is safe. So if you sign up with a cloud phone system, someone will make sure it is authenticated and protected.

This team should be doing regular "horizon-scanning" activities: looking out for new cyber-attacks and making sure your company is ready. If you do not have this in place, a [cybersecurity risk assessment](#) is a great place to start.

Understanding DoS attacks

Every DDoS attack is a DoS attack, but not every DoS is a DDoS. While these attacks are all about overwhelming your system, some are more dangerous than others. By [understanding the latest threats](#) and preparing in advance, you can avoid a disaster that will take out your infrastructure and seriously damage your brand.



Grace Lau

Director of Growth Content,
Dialpad

Grace Lau is the Director of Growth Content at Dialpad, an AI-powered cloud [call center for small business](#) for better and easier team collaboration. She has over 10 years

of experience in content writing and strategy. Currently, she is responsible for leading branded and editorial content strategies, partnering with SEO and Ops teams to build and nurture content. Grace Lau also published articles for domains such as [Agency Vista](#) and [IoT For All](#). Here is her [LinkedIn](#).

Data Privacy Laws: GDPR vs US Data Privacy Laws



BY DR. MICHAEL C. REDMOND, PhD

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR), which came into effect in May 2018, is a set of regulations that create new rights for individuals with respect to their personal data. The GDPR applies to any company that processes the personal data of the European Union (EU) citizens, regardless of whether those companies are based inside or outside of the EU.

The GDPR represents a significant step forward in the effort to establish comprehensive data privacy protections. However, it is important to note that GDPR does not supersede national laws, meaning that companies must still comply with any applicable national laws in addition to GDPR.

Under GDPR, individuals have the right to know what personal data is being collected about them, the right to have that data deleted, and the right to opt-out of its collection altogether. Companies that violate GDPR provisions can be fined up to 4% of their global revenue or \$23 million (whichever is greater).

Comprehensive US Data Privacy Protections

In the United States, there is no federal law that governs data privacy. The reality instead is a myriad of complicated laws ranging from sector-specific, medium-specific, and general open to various interpretations. These regulations apply to the telecom and financial sector along with health and credit information.

Optimism Is On the Horizon

Nonetheless, some optimism is on the horizon, a recently proposed federal privacy law known as the American Data Privacy Protection Act (ADPPA), has shown more promise than its predecessors.



The ADPPA seeks to establish a national standard for data privacy, one that would apply to any company that collects and processes the personal data of American citizens, regardless of whether those companies are based in the United States or not.

The proposed law, alike to GDPR, would give individuals the right to know what personal data is being collected, the right to delete that data, and the right to not allow its collection. It would also create enforcement mechanisms to ensure that companies comply with these provisions,

including fines of up to 4% of a company's global revenue or \$20 million (whichever is greater) for violations.

The ADPPA is still in the early stages of development, and it remains to be seen whether it will garner enough support to become law. However, it represents a significant step forward in the effort to establish comprehensive data privacy protections in the United States.

In the meantime, companies that collect and process the personal data of American citizens should be aware of the patchwork of laws that currently govern data privacy in the United States and take steps to ensure compliance with all applicable regulations.

United States Privacy Laws

The Federal Trade Commission (FTC) serves as a crucial and as the most influential data law enforcement agency in the United States. The Federal Trade Commission Act grants its consumer protection rights authority with broad jurisdiction over commercial entities to prevent unfair or deceptive trade practices. In the past, underfunding and lack of appropriately qualified personnel and resources have limited the scope of their abilities, but that appears to have changed.

They will finally receive an appropriate budget with the necessary personnel and resources to serve as the United States de-factor privacy regulators. The FTC's ability to not only issue regulations but also enforce penalties against organizations that fail to abide makes it a critical component at this particular time. The FTC on behalf of consumer protection can severely punish organizations that fail to follow published privacy policies or choose to mislead consumers by making false security representations etc.

There are also the following federal laws that govern the collection of information online. The Children's Online Privacy Protection Act (COPPA) oversees the collection of information on minors. The Health Insurance Portability and Accounting Act (HIPAA), governs the collection of health information. The Gramm Leach Bliley Act (GLBA), handles personal information collected by financial institutions and banks. The Fair Credit Reporting Act (FCRA), regulates the use and collection of credit information.

The United States maintains a plethora of sectoral data privacy and data security laws among its states. Subsequently, the US state attorneys general supervises



the data governance regulations, such as handling social security numbers and data breach notifications, etc.

Because of the Federal Government's inability to find consensus, it is driving privacy legislation at the state level. Rather than additional delay, state lawmakers have been encouraged by consumers and consumer advocates to take the initiative.

The state of California inspired the domino effect. Four other states have joined to be at the vanguard - Colorado, Connecticut, Utah, and Virginia. They have all executed comprehensive consumer data privacy laws so both consumers and companies know exactly where they stand and have full clarity over important provisions like the right to access or delete information and opting out of the sale of personal information.

Is There a US Version of GDPR?

The General Data Protection Regulation (GDPR) is the most vital data protection legislation enacted at this point in history. It governs crucial criteria, such as the collection use, transmission, and security of data collected from residents of 28 countries, members of the European Union.

The law applies to all EU residents, regardless of the entity's location that collects the personal data. It maintains the authority to issue fines of up to 23 million USD equivalent or as high as 4% of the total global turnover, as mentioned above. Very significant fines indeed ought to serve as a benchmark for a United States framework.


Even though no specific federal data privacy law like the GDPR exists in the United States, however, some national laws were enacted specifically to regulate the collection of data in targeted industries. 1974 brought about the creation of the US Privacy Act governing rights and restrictions of data housed by US government agencies.

The Driver's Privacy Protection Act is another example of data privacy legislation enacted in the United States. This law regulates personal information included in state motor vehicle records.

The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, is a United States federal law that requires financial institutions to explain their information-sharing practices to their customers and safeguards the confidentiality and security of customer information.

The GLBA was enacted in response to the increased





DATA PROTECTION

consolidation of the banking and securities industries. The act repealed parts of the Glass–Steagall Act of 1933, which prohibited any one institution from acting as both an investment bank and a commercial bank.

The GLBA requires financial institutions to develop and maintain a comprehensive security program to protect the confidentiality and security of customer information. The FTC has broad authority under GLBA to take law enforcement actions against companies that it believes have engaged in unfair or deceptive practices affecting consumers' privacy.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is another example of data privacy legislation in the United States. HIPAA regulates the use and disclosure of protected health information (PHI) by covered entities, which are defined as health plans, healthcare clearinghouses, and healthcare providers who transmit health information electronically.

HIPAA establishes national standards for the security of electronic PHI, including physical, technical, and administrative safeguards. Covered entities must also comply with HIPAA's Privacy Rule, which governs the use and disclosure of PHI for treatment, payment, and healthcare operations purposes.

The Children's Online Privacy Protection Act (COPPA) of 1998 is another example of data privacy legislation in the United States. COPPA applies to online service providers that collect, use, or disclose personal information from children under the age of 13.

COPPA requires online service providers to obtain parental consent before collecting, using, or disclosing personal information from children. COPPA also establishes safeguards for the protection of children's personal information, including requirements for data security and data retention.

The FTC has enforcement authority under COPPA and may impose civil penalties of up to \$40,654 per violation.

EU-US Privacy Shield

The EU-US Privacy Shield is a voluntary program that allows companies to transfer personal data from the European Union to the United States in compliance with EU data protection law.

The Privacy Shield sets forth requirements for companies that participate in the program, including a commitment to comply with EU's data protection principles and to provide

robust protections for the personal data of EU citizens. Companies must also provide individuals with certain rights concerning their personal data, including the right to access, correct, and delete their data.

The US Department of Commerce and the European Commission have jointly created a set of Frequently Asked Questions (FAQs) about the EU-US Privacy Shield.

The US Federal Trade Commission (FTC) is the primary federal agency with enforcement authority over privacy and data security issues. The FTC has tools at its disposal to enforce compliance with US privacy and data security laws, including investigations, audits, civil penalties, and injunctions.

The FTC also works with other federal agencies to address privacy and data security issues, including the Department of Homeland Security, the National Cybersecurity and Communications Integration Center, and the Department of Justice.

In conclusion, there are compliance requirements for GDPR and US data privacy regulations. Companies that transfer personal data from the European Union to the United States must participate in the EU-US Privacy Shield program and comply with the FTC's enforcement authority.

When Will the First US Privacy Law Be Enacted?

The likelihood of a single all-encompassing federal data protection regulation imitating GDPR is unlikely in the short term as political entities cannot seem to agree on bipartisanship measures. However, certain states like California have taken up the mantle and introduced their versions of GDPR.

Time will tell whether a US privacy law will eventually be enacted, but in the meantime, companies that handle personal data should assess their compliance posture and make certain they have data handling procedures in place to protect the critical information entrusted to them.

Best practices for companies handling personal data include:

- Developing and maintaining a comprehensive security program to protect the confidentiality of customer information
- Implementing policies and procedures to ensure the proper handling of personal data
- Assessing compliance with data privacy laws and regulations regularly
- Training employees on data privacy best practices
- Working with trusted third-party service providers that have robust data privacy and security practices in place

Enacting a federal data privacy law would provide much-needed clarity and certainty for businesses and consumers alike. It would also level the playing field for companies doing business in the United States, and help to build consumer trust in the handling of their data.

Similar controls between GDPR and US Data Privacy Regulations

- Commitment to comply with data protection principles



- › Enforcement authority over privacy and data security issues
- › Right to access, correct, and delete personal data
- › Robust protections for the personal data of individuals

Conclusion GDPR and US Data Privacy Regulations

- › The EU-US Privacy Shield program is not required for companies transferring data from the EU to the US.
- › The FTC does not have the same powers as GDPR regulators. For example, it cannot impose fines on companies that violate US privacy laws.
- › There is no all-encompassing federal data protection regulation in the US. However, some states, like California, have introduced their own versions of GDPR.



in

Dr. Michael C. Redmond, PhD
 PECB Certified Trainer,
 ISO Cyber Certifications,
 PMP, MBA

Dr. Michael C. Redmond, PhD is a recognized international consultant, auditor, trainer, speaker, and published author. She teaches ISO Certification Courses internationally and has conducted many compliance audits.

Her education includes: PhD (Crisis, Organizational and Behavior Psychology), Integrational Business and Marketing from Fordham University; MBA Risk Management from PECB University; completing Thesis for MBA Information Security from PECB University); Advanced Masters Certificate International Banking and Operations from American Institute of Banking; B.A., Communication Arts & Management from Marymount Manhattan College; Graduate Military Science from ROTC at NYU Polytechnic; Graduate US Army Command & General Staff College; Received GS 12 Rating, Organizational Effectiveness.

Michael spent four years on active duty with the U.S. Army and an additional 17 years in the National Guard and Reserves. Her assignments include Public Relations Officer, Company Commander, and others. She retired at the rank of Lieutenant Colonel.

Michael has three published books that are sold in over 35 countries: Mastering Your Introduction to Cyber Security, Mastering Business Continuity Management, and Mastering Your Work Life Balance.

Her websites are www.redmondworldwide.org and www.solutionfocuscoaching.com

The Importance of Data Privacy

More and more data is processed online during these past decades in comparison to the storing of data on paper and files not too long ago, with the digitalization of processes, from daily life activities to organizational data, like employees, documents, clients information, etc., data privacy concerns started rising.

With the increase of online presence and the use of the internet, the evident truth of keeping your data protected online become more and more prominent, especially during the pandemic where all our work procedures and day-to-day life turned online, from meetings to classes, protecting your data became more important than ever. Gain a better understanding of what you can do to ensure that safety.

Understanding Privacy by Daniel J. Solove



Understanding Privacy demonstrates all the different ways our privacy can be compromised and the potential harm that can come as a result. Providing enlightenment on data privacy threats and its consequences, from identity theft to possible limitations of job opportunities, it brings to light a principled way to face and manage threats, and if possible avoid breaches altogether by understanding vulnerabilities and enforcing security practices. Technology advancements have made it possible for different social media platforms, telephone companies, governments, etc., by using search engines to cater to our personalized interests, mine our information, or track our calls, however, we stay not as informed as we should over our power to be in charge of such technologies and the important decisions we need to make over the collected data, how it is used, or disclosed. A must-read for those who aim to take privacy measures to enforce both, personal and organizational, security.

Data Privacy & Compliance Guidebook: GDPR, CCPA, and Data Privacy Principles by Raj Rathour



A very practical guidebook written in a concise manner to provide a better understanding of Data Privacy Law and to serve as a reference guide for professionals in the field, such as chief privacy or technology officers as well as in-house counsel dealing with organizational data privacy concerns. Aside from being an overview for professionals, this book lays out information in a way that is very easy to understand for beginners in the sector of data privacy. Despite the book's focus mainly being on Data Privacy Law, multiple sections are dedicated to explaining and giving examples of technical aspects of data privacy. As the privacy landscape constantly evolves, so will this guidebook. Even though the guidebook is stand-alone, it may be most useful when combined with the services of a privacy consultant. The privacy professional can anticipate crucial vulnerabilities in an organization by understanding how data breaches occur, through this book, you will be able to gain better insight and examples of detecting vulnerabilities and anticipating data breaches for you and your organization to be better equipped to avoid or manage such situations.

Data Privacy: Principles and Practice by Nataraj Venkataramanan and Ashwin Shriram



Catered to those who lead busy lives with limited leisurely time but a thirst for knowledge on learning more on how to stay secure and protected online, this eBook covers data privacy more in-depth by delving into different aspects of it and providing a better understanding of concepts such as data mining, test data management, synthetic data generation, etc. Anonymization is designed based on data format and discipline and formalizes privacy principles that are essential for good anonymization design. These principles describe best practices and reflect on the conflict between privacy and utility. Viewing it from a practice point of view, it provides researchers and practitioners with a definitive guide on approaching anonymization of multiple data formats, including multidimensional, longitudinal, time-series, transaction, and graph data. Aside from assisting CIOs secure confidential data, it also offers a guideline on its implementation for a wide range of data at an organizational level.

PECB GDPR Implementation Toolkit



The General Data Protection Regulation (GDPR) is a regulation that enforces a stronger data protection regime for organizations that operate in the European Union (EU) and handle EU citizens' data. GDPR establishes the protection of personal data of organizations, employees, consumers, and others. GDPR certification is crucial if you are interested in being equipped with the necessary knowledge to keep your business compliant and ahead of your competitors, as well as assure your customers that you respect their data privacy. Being GDPR certified means that you are legally compliant with the new European Union's Data Protection Regulation (GDPR). GDPR training gives the green light to professionals to receive certification from legitimate certification bodies to prove, both to the EU and the clients, that they are in line with GDPR. The GDPR Implementation Toolkit provides some of the most efficient methods that define roles and responsibilities, as well as instructions on meeting the requirements of this data privacy regime. This toolkit contains a variety of 37 files.

ISO 21502 Lead Project Manager Training Course Available

ISO 21502 aims to help you advance your project management skills and set you on a path to becoming a great project manager by providing guidelines that can help project managers and project-based organizations deliver projects successfully.

This training course helps you develop the necessary competencies for initiating, planning, monitoring, directing, controlling, and closing a project based on the guidelines of ISO 21502.

To learn more, contact us at [**marketing@pecb.com**](mailto:marketing@pecb.com)



How Technology Innovations are Helping in Securing Data

For a very long time, data, whether it was in the form of papers, or it was in the form of bytes and bits on electronic devices, has been one of the most crucial parts of every organization and person. Over the years, the ways data is collected, managed, or processed have changed enormously and technology has played a significant role in this. The more it is growing, and [digital transformation](#) is becoming an integral part of our lives, the more its effects are seen in data.

The evolution of technology and data has changed our lives and has had many positive impacts as it has added convenience, effectiveness, and productivity. In general, it has made our lives easier in many aspects. Among its many benefits, one of the most important ones is how technology has helped in securing data.

The large amount of data exposed online, digital data collected by many organizations, or other data existence, have increased the risk of them being attacked, breached, or destroyed. The causes of such unpleasant events can be different but so can the consequences, from financial loss to reputation damage. In order to reduce and prevent such occurrences, experts are constantly working on developing innovative technology which with help in securing data offering both physical security and cybersecurity.

[Physical security](#) – Various types of technologies can help protect the physical security of data. Physical security refers to the measures designed to protect properties, people, hardware, and software from unauthorized access or other physical hazards.

[Cybersecurity](#) – Refers to the measures taken and technologies used to protect computers, systems, and sensitive information from digital attacks.

Both physical and cybersecurity technologies are needed to protect each other and together secure data by protecting the [three main elements](#) of it which are confidentiality, integrity, and availability.



1. Deterrence – Technologies are used for eliminating or minimizing the risk of security breaches.
2. Detection – Technologies are used to analyze network traffic and data, identify any incident or suspicious pattern, and report before any damage is caused.
3. Prevention – Technologies are used to disrupt breaches, intrusions, or other risky events related to data.

4. Response – Technologies are used to properly respond to incidents that were inevitable.

Just like technology getting more advanced, so is the increasing risks. Criminals have sophisticated their attacking methods and technologies so security experts are being challenged on finding ways to ensure data. But, just like it has increased the probability of corruption, technology innovations are also the main protecting tools when it comes to securing data.



1. Artificial intelligence

Cyberattacks are becoming very complex and difficult to deal with. However, artificial intelligence (AI) is helping with this unprecedented challenge. AI, together with machine learning (ML) are sophisticated technologies that can quickly analyze huge amounts of real-time data and events, hence are able to identify risky behavior and different types of threats. AI technologies are trained to identify patterns, attacks, and weaknesses of different programs and safeguards.

The more data that AI analyzes, the smarter it gets. Machine learning is a subfield of artificial intelligence which enables computers to learn from studying data without being explicitly programmed. This allows for more accurate predicting outcomes. Deep learning is a subset of machine learning. It is a technology that is based on artificial neural networks and uses advanced algorithms to learn from observational data. AI, ML, and deep learning all use their learned information to enhance digital data security.

2. Blockchain

Just like the name explains itself, a blockchain is a chain of blocks, each of which contains information. [Blockchain](#) uses a unique cryptographic fingerprint for each block and a consensus protocol. This allows a secure and tamperproof

way of sharing data that can increase and improve [cloud security](#) by providing transparency, reliability, and confidentiality. Furthermore, blockchain uses encrypted, decentralized, checked data, and multiple nodes on the network, each of which requires confirmation, making blockchain almost impossible to be hacked.

3. Encryption technology

Data encryption is part of the best [data protection practices](#) and one of the most common ones. It is a form of translating data from unencrypted text to encrypted text, and in which information can be only accessed or decrypted by using the correct encryption key or password.

Data encryption can be done using different technologies. Some of the best ones are quantum cryptography, homomorphic encryption, biometric encryption, wearable two-factor authentication, peer-to-peer encryption, widespread end-to-end encryption, lattice cryptography, etc.

Data encryption technologies ensure privacy, security, and integrity. It prevents unauthorized people from reading and intercepting the protected data. Data encryption plays important role in preventing data breaches even if the physical security is compromised.



4. User authentication and authorization

Authentication is a safety process of verifying a person's identity by checking credentials including username and password, but not only. After successful authentication, it starts the process of authorization which determines the verified person's access permission.

Just like many other processes, user authentication and authorization are developing continuously and use more advanced technologies than a simple username and password. Common authentication technologies include:

- Password-based authentication – Even though one of the most commonly used method of authentication, passwords are weaker and more vulnerable to attack than other methods. Although, it does help if more complex passwords are used, and they are not repeated through different accounts and systems.
- Multi-factor authentication – This authentication method requires two or more verification factors to provide access.
- Certificate-based authentication – This method uses digital certificates to identify a user before gaining access.
- Biometric authentication – This security method relies on the use of unique biological characteristics of individuals. Some examples of

biometric authentication technologies involve facial recognition, fingerprint recognition, eye recognition, and voice recognition.

5. Zero Trust

According to the Zero Trust concept, computers, network systems, or humans working on it should not be granted implicit trust. It is a security strategy and its implementation is very complex. Zero Trust is based on three main principles; “Never Trust, Always Verify”, “Implement Least Privilege”, and “Assume Breach”. Zero trust can be implemented through the use of a Zero Trust Network Access (ZTNA) set of technologies.

ZTNA may remind us of another commonly used service which is VPN. However, they differ in many aspects. VPN or Virtual Private Network's main goal is to protect privacy or private network but its use is not enough. While VPNs provide some level of connectivity, zero trust technologies use another approach designed to verify individually every user before providing access.

Other innovative technologies like firewalls, data masking, tokenization, hardware-based security, data backups, resilience, and erasure are helping securing data as well. They are constantly trying to facilitate data security, and to keep up with new trending developments.





TRAINING IN THE OF EU

THE GREEN HEART EUROPE



Training in Luxembourg

As a professional, attending certification trainings comes after searching for a good trainer, which could be checked through his professional experience from his CV or LinkedIn account. Indeed, a non-certified trainer with little to no experience in the field might not deliver added value to the certification course. That was always my focus when I wanted to pass a certification until I came to Luxembourg.

Some fascinating facts about Luxembourg, which I am sharing later in this article, made my experience richer than I had anticipated prior to settling in this country. As a PECB Certified Trainer, I knew that I could deliver more to my clients given what this country offers at different levels.

Being in the center of Western Europe, Luxembourg is an economic hub, not only by its location, but also by the number of big companies, banks, and European institutions, and by sharing borders with France, Germany, and Belgium, Luxembourg attracts businesses, investors, and professionals from all around the world. The exchange of expertise and life experience with people coming from different countries is guaranteed in almost all kinds of events.

A candidate who chooses to attend trainings in Luxembourg will not only take advantage of the trainer's real-life experience but also the diversified professional paths of the other candidates coming from different countries and having worked in different sectors and different companies, like central European banks, public sectors, and big companies who chose their headquarters to be in Luxembourg.

This context made Information Security and Cybersecurity more interesting given the complex business being in place, and of course, the sharp technologies and advanced methodologies used to keep it secure!

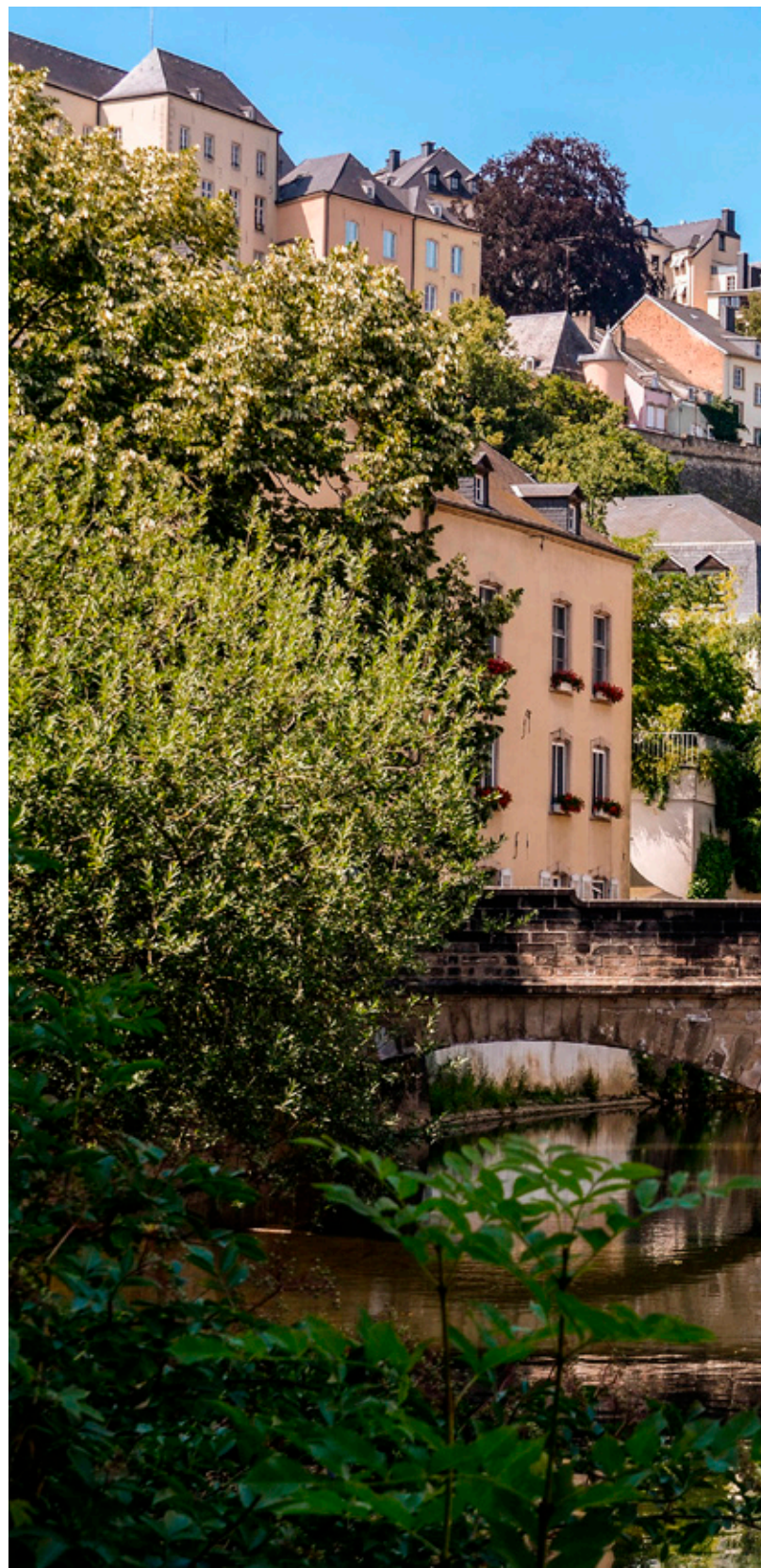
And that was not all!

Transport and Accommodation

Findel International Airport (LUX/ELLX) is the only international airport in Luxembourg. Although it is a small airport, it serves many countries in Europe and outside of the continent. Not far from Luxembourg City, the airport can be reached by car, bus, and taxi.

A big number of hotels of different ranges are available across the country offering different pricing to match high and limited budget. There are hotels just next to the Airport which is reassuring for people bringing heavy luggage or for those who do not trust public transport to catch their flight.

The country of Luxembourg highly encourages people to use public transport. And so do we. Besides the many



known benefits for climate change, public transport in Luxembourg is one of the best ways to explore the country as it is very fast, and since 2020, it is also free throughout the entire country.

A Visit to Enjoy

The list of places to visit when visiting Luxembourg is endless. Whether you are more interested in history,

science, or have other interests, you can find many places to visit and enjoy.

Historic Landmarks

Even though a small country, over the years, Luxembourg has a rich history dating back to the 10th century. Influenced by many cultures and eventful history, Luxembourg is home to many fascinating historical attractions.



1. Casemates du Bock

The Bock rock and the casemates are a series of underground tunnels and passageways approximately 23 km long, built for protection purposes. It has been a UNESCO World Heritage Site since 1994 and it is visited by over 100,000 tourists every year. This must-see attraction provides visitors with a unique experience different from other conventional tours allowing them to delve into the history of the county.



2. The Grand Ducal Palace

The Grand Ducal Palace is the official town residence of the Grand Duke of Luxembourg. He and the Grand Duchess, and their staff, have their offices in the palace. Besides being used by the Grand Duke to perform his official duties, the palace is also used for a variety of meetings, to accommodate important guests like foreign heads of state, and it is also used as a venue for many state ceremonies and official receptions. The palace is also known for its magnificent, unique, and beautiful façade.

3. Château de Bourscheid

The charming Castle of Bourscheid is the biggest castle in Luxembourg and has an impressive structure with characteristic round towers. It is believed that the castle was built around the year 1000 as a part of the Holy Roman Empire. Besides being beautiful itself, standing 150 meters above the River Sure, the castle is surrounded by picturesque views as well. In the evening, the building is illuminated looking like a fairy-tale castle.



4. Vianden Castle

As one of the largest and most beautiful feudal residences from the Romanesque and Gothic eras, Vianden Castle is one of the most popular tourist attractions in Luxembourg and one of Europe's leading historical monuments.

During their visit, tourists can enjoy the beautiful exterior and interior of the castle, and also the amazing view of Northern Luxembourg.



6. Esch-sur-Sûre Castle

Located in a small town with the same name, Esch-sur-Sûre is a ruined castle whose foundation dates back to the year 927.

Even in this condition, the castle still manages to offer a fairy-tale-like atmosphere. In addition, the beautiful surrounding mountains and river make the view even more fascinating.



5. Clervaux Castle

Laying in a valley between forests, the white Clervaux Castle immediately catches the visitor's attention and takes over the rest of the city.

Clervaux Castle dates back to the 12th century, however, being destroyed during the Second World War, the castle was fully restored afterward. The castle is home to several museums and exhibitions, including here the famous "The Family of Man".



Museums in Luxembourg

There are more than 60 museums in the Grand Duchy that enable visitors to explore the history, culture, and heritage of Luxembourg. Among many museums, here are some of the most popular ones:



1. Luxembourgish Aviation Museum

Visit Luxembourgish Aviation Museum and discover many model aircrafts, historical parts, and accessories from Luxembourg's fascinating aeronautical heritage. Immerse yourself in the world of aeronautics developments and get introduced to different disciplines like motorized and gliding aviation, parachuting, etc. See the oldest wooden plane to have flown in Luxembourg in 1946 and the first hot-air balloon. Moreover, learn how weather stations work, how a conversation between the pilot and the control tower sounds, and explore the centerpiece of the museum, the "Klemm".

2. National Museum of History and Art

Situated in Luxembourg City, the National Museum of History and Art is a perfect place to visit many artworks and artifacts from all periods of Luxembourg's history. The museum has a lot to offer to its visitors including themed exhibits, permanent coins and medals collection, and many archaeological artifacts.

3. Mudam Luxembourg Modern Art Museum

Mudam Luxembourg or Musée d'Art Moderne Grand-Duc Jean is a museum of modern art in Luxembourg City that opened in 2006 in a spectacular building. Its main mission is to present the most relevant art of the time by displaying current artistic trends.



4. Lëtzebeurg City Museum

The Lëtzebeurg City Museum is a wonderful place to see a thousand years of Luxembourg City's history brought back to life. Through many spectacular displays and multimedia animations, the museum has found the perfect interactive approach to highlight the key historic moments of the city.



5. Casino Luxembourg

Located in the heart of the city, Casino Luxembourg Forum d'art contemporain was founded in 1996. Since then it has been holding many international contemporary art exhibitions. The museum has combined art with a warm and friendly atmosphere, making it welcoming for everyone.

Things to Do in Luxembourg

Besides falling in love with the history and culture of Luxembourg and admiring the architectural masterpieces, there are many other exciting activities you can do during your stay in Luxembourg.

Hiking

Luxembourg has many fascinating hiking trails and it is an ideal destination for nature lovers. Among these trails, some of the most famous ones are:

- 1. Mullethal Trail** – Located in the Mullerthal Region, also known as Luxembourg's little Switzerland, this trail is 112 km long and has three main trail routes, each characterized by its own uniqueness. The first route is rich with rocks, woods, and meadows. The second route brings hikers to fascinating rock formations in the heart of Mullerthal. The third route not only has man rocks, but also many romantic castles and enchanting stream valleys.
- 2. Echternacher Wollfsschlucht** – This 13.4-long trail along the German-Luxembourg border is great for camping and hiking. It is considered to be one of the most interesting trails in Luxembourg surrounded by great views of impressive rock formations.
- 3. Escapardenne Lee Trail** – This over 50 km long-distance trail runs through dense forests and river valleys. It offers breathtaking landscapes and it is ideal for hikers seeking adventures.
- 4. Manternacher Fiels** – is a nationally protected area and a certified premium hiking trail. The center of this area covers 57 hectares and is the largest canyon forest in Luxembourg. Human intervention in the forest area is very limited and it has not been cultivated for about 50 years. While walking on this trail, you get to enjoy the view of many beautiful forests, water sights, and impressive rocks.



Running

Do you love running? If yes Luxembourg will take really good care of you by offering good and fun running activities. The stunning views definitely call for some sight running tours.

- 1. Luxembourg 'Runseeing' Tour** – This 10 km running loop is an incredibly fun way of exercising by seeing some of Luxembourg's best sights at the same time. The route starts near the Central train station and heads towards the Pont Adolphe Bridge where you can enjoy the view over the Petrusse valley. The trail also takes you to other parts of the city where you can run alongside two river paths. During the run, one also gets to see many important monuments. The runners can also climb during a part of the trail or they can choose to use the Pfaffenthal lift to rejoin the route later on top.
- 2. Wenzel Circular Walk** – This run will take start at the Bock Promontory which is the rock on which Luxembourg City was first built. Visitors get to see the oldest parts of Luxembourg City, some beautiful nature views, and many great buildings, among which is the Chemin de la Corniche, which is also referred to as the most beautiful balcony in Europe. The entire Wenzel Circular Walk is 5.5km long, however, you can also choose to run longer distances using other paths and streets.
- 3. Parc Municipal and Parc Merl-Belair** – Luxembourg City has many gorgeous and lovely parks and this run will get you to two of them: The Municipal Park and the Merl-Belair Park. Even though in a fairly short and flat route, the run will be very pleasant and the views are magnificent.

- 4. Petrusse Valley Parks** – This run will take you away from the city's business and will get you to a calming park hidden in the city. The route will allow you to see impressive fortification ruins and other “strange” rock formations.

Cycling

Having 600 km of cycling routes and more than 700 km of mountain bike trails, Luxembourg makes a great place for cycling enthusiasts. Whether you are a professional biker, or cycling is just a hobby for you, Luxembourg offers delightful rides for everyone and amazing landscapes. A very famous cycling group is The Velosvedettes who is also known as the “Spice Girls” of Luxembourg’s cycling world. This group is amazing for those who want to experience outdoor fun while becoming part of communities and creating new friendships.

Water Activities

Among many activities, the Grand Duchy is also known for hosting many water activities. Having lots of streams, lakes, and amusement parks, it is a great place for having fun water experiences. Two of the most well-known water and amusement parks highly rated by travelers on TripAdvisor are AquaPark Kaul and Schueberfouer.

Depending on your hobbies and preferences, in Luxembourg, you can do numerous water activities and pleasures like riding in a calm and peaceful passenger boat or riding a speedy and adventurous motorboat, both of which will be done while admiring the green breathtaking mountains surrounding the river. Moreover, you can go for a session of wakeboarding, which is like waterskiing, and



do not worry, you do not have to be an athlete to do that. Canoeing and kayaking are some other unforgettable fun ways to discover the beauty of Luxembourg’s rivers and even the plant and animal life.

Pedalo is another water exercise that you can try with your friends and family. A famous place for doing pedalo in Luxembourg is Echternach, the oldest town of Echternach. Having many species of fish, Luxembourg is also the perfect place for fishing, however, you do need a fishing license first. Another adventurous water activity that you can do in Luxembourg that is really trendy is the stand-up paddleboard. A fabulous place for this sport is Upper Sure Lake.

We have not forgotten about swimming either. Luxembourg has many lovely beaches where you can enjoy the sun, the flora, and the cool fresh grassy areas to cool down, and you can have fun swims. Swimming in the clear water surrounded by amazing views is an unforgettable way to spend high-temperature days.

Local and International Food

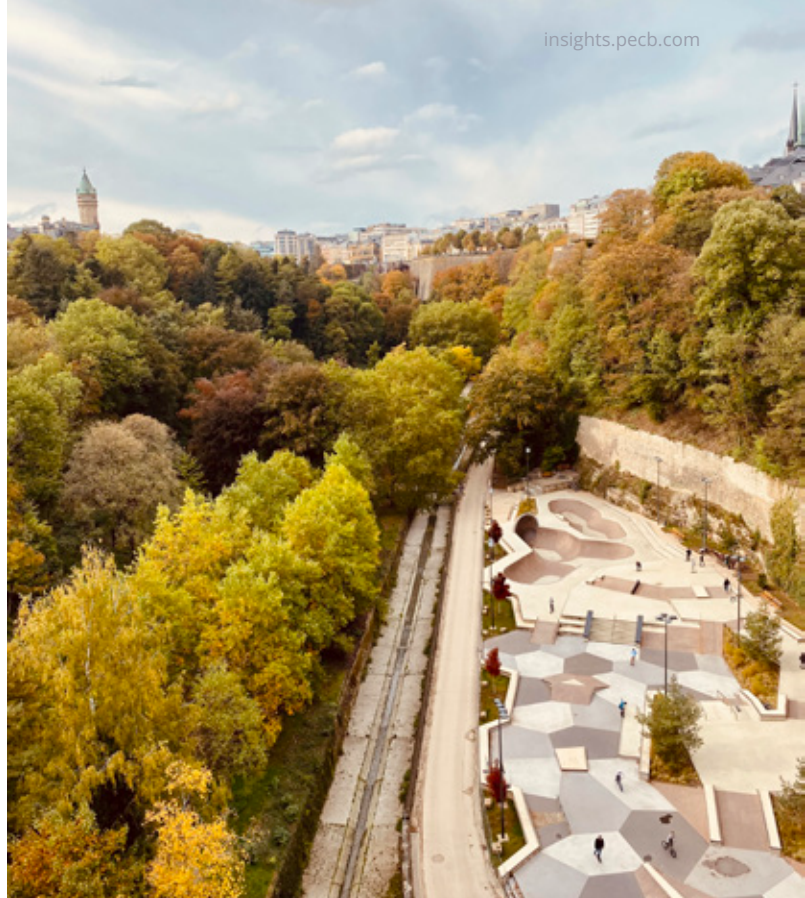
Luxembourg has its own cuisine, a delicious one of course. Some of the famous local meals are Bouneshclupp, a green bean soup, is one of Luxembourg’s specialties usually served with Gromperekichelcher (potato pancakes), Rendfleischbitt (beef broth with vermicelli), and Gromperenzopp (a potato soup with leeks, egg yolks, and cream).

Besides, you can find literally all kinds of cuisines. By walking in the city, you can easily find Italian, Japanese, Chinese, French, Moroccan restaurants, and the list is very long. No matter what the allergy or diet is, there is a restaurant to care for that. This can easily be checked through Google and the restaurants websites.

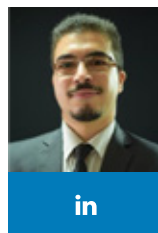


Facts About Luxembourg

- Luxembourg is one of the safest countries in the world.
- Luxembourgers are typically tri-lingual, with the country having three official languages: German, French, and Luxembourgish or Lëtzebuergesch.
- Luxembourg is the only remaining Grand Duchy in the world with a Grand Duke as head of state.
- Luxembourg is a landlocked country bordered by Belgium to the West, France to the South, and Germany to the East.
- Luxembourg is the richest country in the world, with a PPP per capita value of \$118,503.6. The small country is one of the major economies in the Eurozone.
- It had the largest gross domestic product (GDP) per capita in the world in 2014 at \$111,716 based on the International Monetary Fund's World Economic Outlook Report in April 2015.
- The entire country's population is approximately 525,000 and 43% of which are foreign residents. It has the highest number of expats among European countries.



- Luxembourg is among the twelve founding member countries of the North Atlantic Treaty Organization (NATO).
- Luxembourg was also among the six founders of the European Union together with Belgium, France, Germany, Italy, and the Netherlands.
- Skype's corporate headquarters, as well as the European headquarters of Amazon, Paypal, Rakuten, and Rovi Corp. are based in Luxembourg because it is a known strong financial center and tax haven.
- Public transport including buses, funiculars, tramways, and trains are totally free within the country.
- One of the country's most famous attractions is the Bock Casemates, a 21-kilometer underground tunnel network.



Abdelmalek Najih

Founder & CEO at AN Advice
Goup IT Security Compliance
and Threat Intelligence Officer
at IQ-EQ Group

Abdelmalek Najih is an Information Security Expert. He has been working as an auditor, adviser, and trainer in the field of information and cybersecurity with clients in various sectors in different countries in Africa and Europe. Mr. Najih's expertise are mainly oriented toward information security governance, risk, and compliance.

Cybersecurity Awareness Month

With the increase in internet usage constantly, especially during COVID-19, the need to better understand cybersecurity has become evident. We are learning the importance of our cyber safety and becoming more aware of potential threats or malicious acts by the day.

Since 2004, **Cybersecurity Awareness Month** has aimed to help individuals protect their online presence.

This year's theme is See Yourself in Cyber, in an effort to educate people on cybersecurity, who deem it a complex subject, however, it is all about individuals and organizations making smart and well-informed decisions on all aspects of their job, home, or even school.

This campaign encourages all to do four simple steps to better ensure their cyber safety:

1. Enable Multi-Factor Authentication



2. Use Strong Password



3. Recognize and Report Phishing



4. Update Your Software



Do you want to learn more about cybersecurity? Be a cybersecurity expert? How to avoid online threats? How to stay protected from malicious acts? You can learn more in-depth through our cybersecurity training courses!

Explore Cybersecurity





Happy Worlds Standards Day

We all want a better world, one that can be enjoyed today and enhanced for future generations.

The Sustainable Development Goals (SDGs) represent a shared vision for peace and prosperity, for people and the planet. Every SDG is a call for action, but we can only get there together.

We all seek more security, sustainability, and fairness. International Standards were developed with the purpose of creating that bridge and offering practical solutions, for organizations and individuals, so we can work toward a better today and become part of the solution. We all need to do our part to help.

PECB offers training courses that reflect the latest standards, technologies, approaches, most innovative methods, and practical examples.



FIND OUT MORE ▶



ISO 37001 Lead Auditor eLearning Training Course Is Available in English!

PECB is excited to announce that ISO 37001 Lead Auditor eLearning training course is now available in English.

CHECK THE BROCHURE!

To learn more about our other eLearning training courses, please [click here](#).

WEBINAR **LIVE**

KEEP AN EYE OUT FOR OCTOBER'S WEBINAR

Cybersecurity risk management is a strategic approach that helps organizations prioritize threats.

This approach guides the organization in identifying, analyzing, evaluating, and addressing the threats based on the impact of the potential threat.

TOPIC: ISO/IEC 27032 vs. ISO 31000 – How do they help towards Cybersecurity Risk Management

October 12, 2022 at 3:00 - 4:00 PM CEST.



SHERIFAT AKINWONMI

Experienced Cybersecurity Professional



GEARY SIKICH

Sr. Crisis Management Consultant,
Author and Business Advisor



REGISTER HERE

Data Privacy Automation – What You Need to Know



BY RAMESH KUMAR PRABHAKARAN

The Need for Data Privacy Initiatives

The US has seen many States coming up with their own Data Privacy regulations in recent years. Data Privacy is a growing concern for organizations worldwide, who are faced with an increasing number of Data Privacy regulations governing their collection, use, processing, storage, and disposition of personal information about their consumers and employees. Although the modern Data Privacy regulations started in Europe with the advent of GDPR, the trend is quickly catching up in North America and other locations around the world.

Enforcement authorities for Data Privacy regulations could impose huge fines on those companies who do not comply with them. General Data Protection Regulation, for example, could impose up to 20 million EUR or four percent of worldwide turnover. Hence, large organizations are now increasing their IT budget toward Data privacy initiatives to avoid the penalties and other negative implications of non-compliance.

One of the important requirements of many Data Privacy regulations worldwide is that organizations need to provide their customers with the right to request access, correction, and deletion of personal information held by them. This requires organizations to build capable systems that could help review and respond to Data Privacy related requests from their consumers.

While embarking on these initiatives to comply with Data Privacy regulations, organizations are typically faced with two options. The first option is that they could choose to build the necessary systems from scratch by themselves leveraging existing enterprise-wide processes and systems. The second option is that organizations could buy licenses for relevant commercial off-the-shelf tools available in the market and customize the tools for their specific organizational requirements and priorities.





Build Your Own Solution

This option is more popular among organizations looking to reach a minimum defensible position by a specific compliance deadline. This minimum defensible position may mean different goals for different organizations depending on their risk appetite and level of exposure to regulatory requirements.

One of the advantages of this approach is that this helps organizations to start with a lower-cost solution and then decide about investing in a full-fledged solution later depending on the volume of Consumer and data subject requests received by the organization. The "Build" option also allows these companies to leverage their existing IT capabilities to create their Data Privacy solution.

For example, if the organization is already using SharePoint, then the workflow capabilities within SharePoint could be used to build a data Subject and Consumer request management system. However, one of the disadvantages of this approach is its scalability. This approach could end up consuming more time and efforts of internal IT

departments in the long run, if and when the volume of consumer and data subject requests crosses a threshold and organizations find themselves needing to invest in a more sophisticated solution.

Commercial Off-the-Shelf Solution

This option is typically more suitable when an organization is looking at Data Privacy initiatives with a long-term view rather than just looking for a minimum defensible position to avoid the penalties for non-compliance. This option involves buying a license for one of the commercial tools available in the market for Data Privacy and Data Governance. These external tools are typically more expensive than home-grown solutions but can seamlessly scale for a higher volume of consumer requests with maximum efficiency. These tools also typically provide end-to-end Data Privacy solutions covering consent management, consumer request, and record of processing. The major disadvantage of the solution is the high annual license cost associated with using the tools, in addition to the maintenance costs.

Data Minimization

One of the core principles of modern Data Privacy Regulation such as GDPR is the need for Data Minimization and Privacy by Design. It is expected that most regulations worldwide will evolve to include data minimization, and hence, it becomes a key area of interest for organizations embarking on Data Privacy initiatives even if the current regulatory requirements do not call for the same.

Data minimization requires organizations to collect only the minimum amount of personal information from their consumers, as needed for legitimate purposes for which they are required, and to store this information only for as long as they are necessary to fulfill legitimate business or legal requirements. This in turn calls for organizations to design and implement data retention policies, which are appropriate to the nature of personal information and the purposes for which they are being processed.

Challenges in Implementing Data Retention Policies

Deletion of specific consumer information according to its retention policy schedule poses a great challenge because of the potential database integrity constraints and the impact on upstream and downstream applications. To mitigate this challenge, organizations are advised to craft comprehensive data lineage of their IT architecture and assess the flow of personal information starting from the source to all downstream systems. There are a lot of commercial Data Discovery tools available in the market that help in this exercise but they require that all the internal data sources to first be connected to these tools

before they can provide data lineage reports. Yet, this does not solve the problem totally, as deletion of consumer information should also factor in the need for exceptions to retention schedule for various purposes, such as legal hold, regulatory requirements, business purposes, etc.

Scope for Automation in Solving Data Retention Puzzle

As a result of the complications involved in data retention, even the leading Data Privacy tools in the market have not been able to effectively design a data retention solution, which could seamlessly implement the enterprise-level data retention policies. At this point, most organizations are, therefore, adopting a largely manual approach in assessing the data lineage and validating for database integrity constraints. Organizations are still trying to automate the process to the extent possible by creating deletion scripts that check for retention policies and carry out the deletion of personal information that is past the retention schedule.

Commercial tool vendors, on their part, are also trying to create solutions that could improve the efficiency in largely manual processes of implementing Data Retention. For example, once all data sources are connected, many commercial tools can catalog personal data into profiles that can be searched through a centralized interface. Once the data retention schedules are also defined in the catalog, certain commercial tools could analyze the catalog and flag the candidate data for deletion to the respective business or system owners. The downside of the solution is the actual review and deletion of candidate data flagged for deletion which is a responsibility of the respective IT system owners and is largely a manual process. Naturally, there is still a lot of scopes to bring in more avenues for automation to solve the Data Retention Puzzle.



Ramesh Kumar Prabhakaran
Consultant – Data Privacy

Ramesh is a Data Privacy consultant and has over 9 years of experience in the IT industry playing diverse roles involving Consulting, Business Analysis, and Project Management.

Ramesh has expertise in Data Privacy regulations, such as GDPR and CCPA and leading Data Privacy technologies. Ramesh has helped clients across Europe and US in advising and steering the end-to-end implementation of Data Privacy initiatives starting from assessment, Data Discovery, and building Data Privacy solutions.



Top Five High-Paying Job Positions You Can Pursue with an ISO/IEC 27701 Certification

In an era when most people have access to and use the internet, organizations all over the world collect and manage a large amount of personal information and other data on daily basis. In an ideal world, all this data collection would be used to improve the customer experience for organizations and their clients. There are, however, several malicious activities and cybercriminals that pose a substantial threat to data and privacy security.

Data breaches continue to affect organizations and customers all over the world. A worldwide study conducted by [Tech.Co](#) found that organizations suffered an average cost of \$4.35 million due to data breaches this year, which represents a 2.6% increase over the previous year. Attacks like this can be very damaging to an organization, but not only financially wise, they can also affect their employees, customers, and reputation. To be protected from such attacks, organizations should take preventive measures and implement a privacy information management system (PIMS).

[ISO/IEC 27701](#) is a globally known standard that identifies guidelines and requirements for establishing, implementing, maintaining, and improving privacy information management. Considering the high need for a successful implementation of the PIMS, organizations all over the world, are in high need of professionals who have relevant competency, expertise, and skills. The PECB ISO/IEC 27701 training course will help you understand how to implement the requirements and guidance of the ISO/IEC 27701 standard in your organization along with its benefits.

1. Chief Privacy Officer (CPO)

According to *Salarycom*, *PayScale*, and *Glassdoor*, the average U.S. annual salary of a Chief Privacy Officer is **\$177,590**.



2. Privacy Director

Based on the information provided by *Salarycom*, *PayScale*, and *Glassdoor*, the average U.S. annual salary of a Privacy Director is **\$145,046**.

3. Privacy Engineer

According to *PayScale*, *ZipRecruiter*, and *Glassdoor*, the average U.S. annual salary of a Privacy Engineer is \$131,276.

4. Privacy Manager

According to *Salarycom*, *ZipRecruiter*, and *Glassdoor*, the average U.S. salary of a Privacy Manager is \$112,549 per year.

5. Privacy Analyst

According to *ZipRecruiter*, *PayScale*, and *Salarycom*, the average U.S. salary of a Privacy Analyst is \$84,111.

The ISO/IEC 27701 family such as ISO/IEC 27001, ISO/IEC 27005, ISO/IEC 27032, Cloud Security, etc., assists you in understanding the practical approaches that are involved in the implementation of an information security management system (ISMS) that preserves the confidentiality, integrity, and availability of information.

ISO/IEC 27701 opens the door to a wide range of opportunities to individuals who want to make a career in protecting their organization's data privacy from various malicious attacks and cybercrimes.

Note: The salaries of the above-mentioned positions are not definitive and they may change with time and industry development.

[CHECK OUT THE BROCHURE!](#) ▶





PECB UNIVERSITY
EXISTIMATIO PER VERITATEM

A First-Hand Experience of Studying at PECB University



Through this interview, B.M. Zahid-ul Haque shares his experience at PECB University studying MBA in the Information Security Management program.

How has the studying experience at PECB University helped you in your work settings?

My studying experience at PECB University was great. It has had an effective direct impact on my work setting. It helped me to advance my competencies in relation to information security, cybersecurity, and business risks, and learn more profound ways to manage cybersecurity challenges technically and strategically by constantly considering the business aspects. I was able to learn deeper about how to detect and mitigate security threats, conduct a cybersecurity management system, and develop and implement adequate cybersecurity practices that allow an organization to protect information assets.

As I am responsible for cybersecurity, I need to set a goal for the cybersecurity strategy of the organization which must be aligned with business objectives. This course has helped me to gain better technical knowledge of cybersecurity and a greater understanding of how the business world meshes with cybersecurity. It has imparted to me a strong business acumen and made me understand better the business and financial implications of technical decisions and overall strategy.



What is one thing that you like about your studying experience at PECB University?

My MBA in the Information Security Management course was very unique. I found the course curriculum and the faculty members are top-class at PECB University. Generally speaking, both soft skills and hard skills are needed to succeed in a career. The combination of business courses, specialized courses, elective courses, and practical capstone projects helped me to advance both my leadership and technical skills. The study method was excellent. Moreover, multiple global professional certifications in critical cybersecurity domains and standards, as a part of the course, have gained further acceptance and helped me to become a confident leader in the Information Technology and Risk-Management sector.

What message would you give to future PECB University candidates and students?

It is necessary to take the quality decision at the right time because it leads to success. PECB University has a practical-oriented modern curriculum, which can boost your career's success. Remember that "Setting goals is the first step in turning the invisible into the visible."



PECB UNIVERSITY

EXISTIMATIO PER VERITATEM

The class of 2020 at PECB University has graduated from their EMBA programs. This is a result of their hard work and dedication toward their goals. It is evidence of their academic and professional education through numerous courses and effective development, implementation, and management.

We wish the students the best in their professional and academic paths onwards.

Join the PECB University family. Visit the PECB University [Website](#) to get better informed or contact the PECB University counselor at university.studentaffairs@pecb.com





REINFORCE YOUR EXPERTISE, FOR BETTER OPPORTUNITIES

Make the most of PECB's new and updated training courses!
Contact us at marketing@pecb.com or visit our [website](#) for more.

New and updated training courses

Training Course	Language	Status	
ISO 21502 Lead Project Manager	English	Updated	→
ISO/IEC 27002 Manager	English	Updated	→
ISO 22301 Foundation	English	Updated	→
ISO/IEC 27001 Foundation	English	Updated	→
ISO 37301 Lead Implementer	English	Updated	→
ISO/IEC 27001 Lead Implementer	Spanish	Updated	→
ISO 37301 Foundation	French	New	→

GET WELL-VERSED IN YOUR CHOSEN FIELD

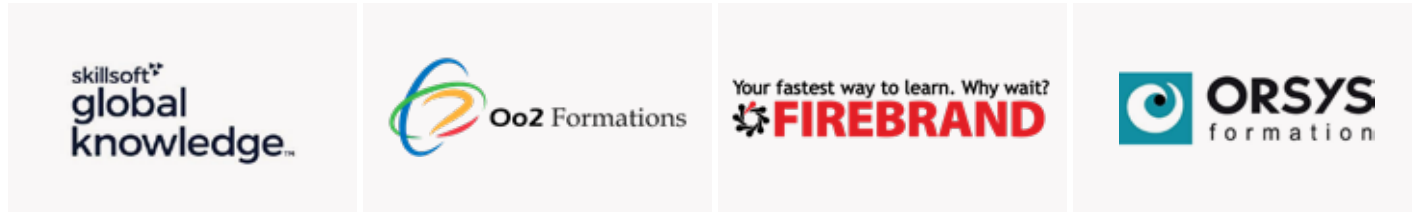
Open your doors in the field of your interest through the PECB Store, where you will be able to find the knowledge that you need to enrich your experience.

PECB Store offers a variety of ISO standards, training courses, toolkits, and much more to boost your professional journey in your chosen career path.

HAPPY SHOPPING! ►

SPECIAL T

TITANIUM



GOLD PA



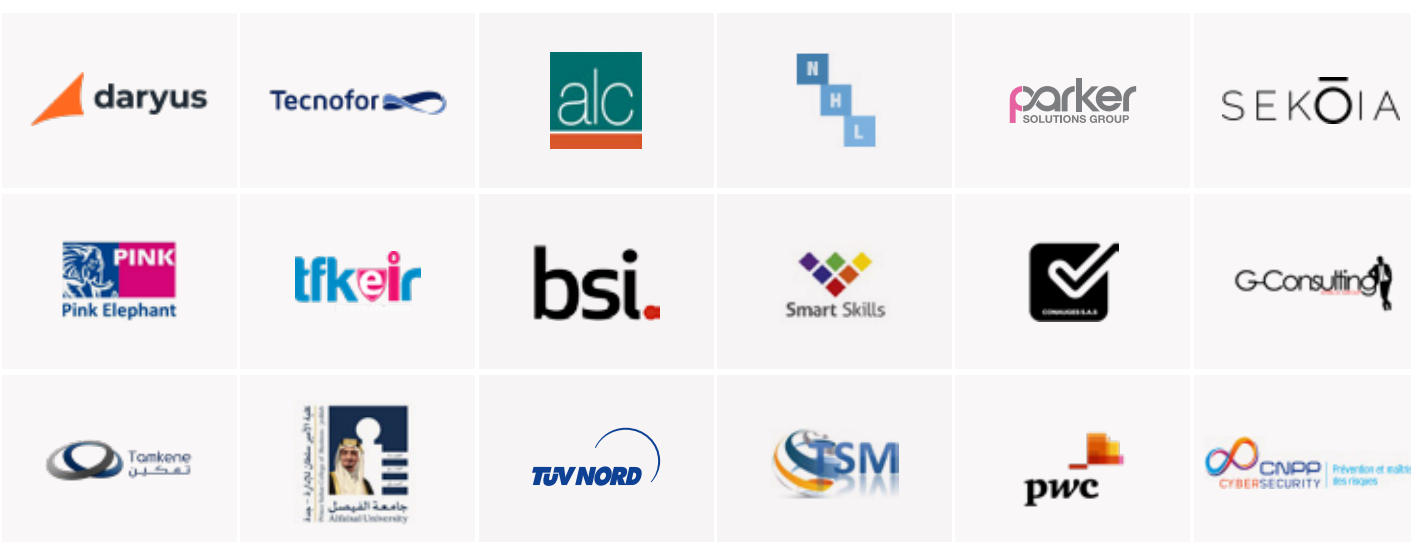
Note that PECB Partners are listed as per the credits

HANKS TO

PARTNERS



PARTNERS



**STRENGTHEN
YOUR
ORGANIZATION'S
SECURITY WITH
ISO/IEC 27701**

