ECS
EUROPEAN CYBER SECURITY ORGANISATION

AUGUST EDITION
AWARENESS CALENDAR

Privacy & data security

Awareness Calendar **CYBERSECURITY**

This calendar will feature a different topic each month to spread awareness of key aspects of cybersecurity and showcase ECSO Members' and Partners' solutions and services in the relevant areas to potential users.

The monthly themes for 2022 are planned as follows:

- January – Cybersecurity certification
- February – Internet of Things
- March – Gender diversity in cyber
- April – Artificial Intelligence
- May – Cyber ranges & range-enabled services
- June – Cybersecurity for verticals
- July – Social engineering
- August – Privacy & data security
- September – Organisational resilience
- October – Cyber hygiene & readiness
- November – Cloud computing
- December – Threat & vulnerability management

DID YOU KNOW?

- The EU Charter of Fundamental Rights stipulates that EU citizens have the right to protection of their personal data. The General Data Protection Regulation (GDPR) covers the protection of natural persons with regard to the processing of personal data and on the free movement of such data. The regulation is an essential step to strengthen individuals' fundamental rights in the digital age and facilitate business by clarifying rules for companies and public bodies in the digital single market. READ MORE.

- The European Commission published on the 25th May 2022 Questions and Answers (Q&As) to provide practical guidance on the use of the SCCs and assist stakeholders in their compliance efforts under the General Data Protection Regulation (GDPR).

ECS

EUROPEAN CYBER SECURITY ORGANISATION

RESOURCES FROM OUR MEMBERS

(ISC)² offers several options for cybersecurity privacy and data security

(ISC)² offers several 1-hour security briefing webinars specific to cybersecurity privacy and data security, providing an opportunity for attendees to take a "deep dive" into a specific cybersecurity related topic and to learn from industry experts.

Privacy: Ransomware Resilience: Build a Holistic Data Protection Strategy
Planning for COMPLETE Recovery from a Ransomware Attack
Privacy Regulation Roadmap Training Course – In this course participants will examine global privacy legislation and learn the importance of identifying and complying with privacy laws and regulations that apply to your industry and customer base.

Data Security: The Future of Security Operations: Strategies from Successful Leaders
Holistic Application Security for PCI DSS Compliance
Stop Threats Earlier by Integrating NDR and Other Cybersecurity Solutions
Use a People-Centric Defense to Build Resilience to Today's Cyber Threats
Second Order Cyber Risk: Exposing Your Blind Spots
(ISC)² comprehensive article on The Importance of Adopting a Risk Management Approach to Security and Privacy

Accenture data security and privacy

To meet their clients' unique security expectations and address today's dynamic regulatory issues, Accenture's Information Security team operates a global Client Data Protection (CDP) programme. This programme provides client engagement teams with a standardised approach, the security controls and tools necessary to the keep data safe. Accenture's CDP process begins with the initial client conversation, where they try to identify any inherent risks or security concerns. These collaborative talks also focus on identifying and mitigating potential weaknesses within the client environments, clarifying accountability and removing any ambiguity. The results of each risk assessment and client discussion are then factored into Accenture's solutions so that they ensure security from the start. Through regular assessments and refinements to the CDP programme, and a workforce that takes accountability for putting security first, Accenture continues to improve how they protect the data of their organisation and operations, and that of their employees and clients.
READ MORE: Accenture privacy statement & Keeping client data protected

Digital Feng Shui

The Cybersecurity Agency of Catalonia, through the Safer Internet Program, is launching a campaign to help citizens protect their data.

The goals of the campaign are:

- Warning citizens about risky daily digital behaviours regarding data protection.
- Providing the necessary tools and training for citizens to help them reach the needed technological knowledge to protect their information.

Digital Feng Shui will feature web articles alongside a few podcasts with easily understandable practical tips. All content will be posted on their official website.

By @internetambseny @ciberseguracat #ECSO #cyberawareness

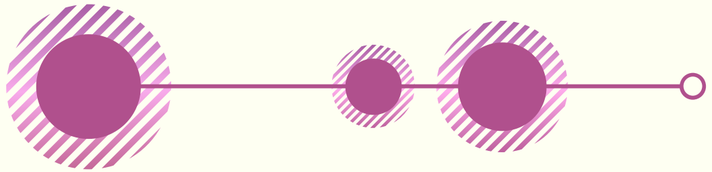
READ MORE. (in Catalan)

How to protect your privacy online

In the last decade, not only big companies but also individual users have suffered countless data breaches, information leaks, phishing attacks, and other online hazards. In our everyday lives, we routinely check for traffic before crossing a street: we should practice everyday safety awareness in the same way for our digital lives, as well.

To maintain data security and protect our privacy, we have to take care of our accounts and devices and bravely consider – and prepare for - the potential of a worst-case scenario: a major data breach.

Security and privacy are interconnected: we need to adopt similar best practices to protect both. To stay safe and hold cyberattacks at bay, APWG.eu has prepared the following recommendations for protecting your privacy online. READ MORE.



ERICSSON

Cryptography and privacy: Protecting private data

The worlds of cryptography and privacy are equally exciting and urgent, having grown in the wake of digitalisation and cloud computing. Predications indicate they will impact all aspects of our modern digital life. But how do these worlds connect? And what about privacy-enhancing technologies? This blog discusses how cryptography can provide us with the tools necessary to make the processing and communication of private data secure.
READ MORE.

Cybersecurity compliance: Data-centric privacy and security

The obligation to comply with the GDPR (General Data Protection Regulation) represents an opportunity for growth for your organisation.

From the various innovations in the regulations, such as the right to be forgotten, the need arises to create new roles and to access profiles and visibility rules. Furthermore, it is appropriate to consider the need to adapt the applications involved, without affecting the already operational functionalities and structures in the company, in accordance with the new GDPR requirements.

The solutions adopted by Exprivia Cybersecurity are equipped with features focused on applications such as: automatic and guided "Discovery", "Redaction", "Dynamic Masking" to implement the minimisation rules, "User Profiling and Continuous Monitoring" and "Logical & Physical Deletion". These features allow the company to have the answer to all the GDPR requirements for its custom and off-the-shelf applications in a single solution. READ MORE.

uTile: Health data processing cryptography

Within the Ministry of Economy and Enterprise's Digital Enabling Technologies program, GMV is developing the use case related to the comparison of the efficacy of clinical treatments in which hospitals, healthcare centres, research centres, and pharmaceutical industries need to collate health outcomes to obtain better conclusions as to the effectiveness of treatments. However, patient data is specially protected by the GDPR, complemented in Spain by the Law on Patient Autonomy. With uTile, useful information such as survival, biomarker value, prognosis, the average age of patients, etc., of clinical treatments can be shared, facilitating GDPR compliance. READ MORE.

Data anonymisation in Big Data scenarios: A risk-based approach

gradiant
Connectivity · Intelligence · Security
for your business

The arrival of Big Data played a significant influence in the rise of worries about data privacy, specifically how personal data is acquired, processed, and for what purpose. Data anonymisation is one mechanism for improving individual data privacy. When implemented right, anonymisation makes it impossible to identify a specific individual in a dataset. GRADIANT has developed an automatic data anonymisation solution to improve privacy while retaining the data's usability for use in analytical tasks. We take a risk-based approach, allowing data owners to customise a set of anonymisation methods as well as privacy and utility metrics. The tool computes different combinations of anonymization tasks while assessing achieved privacy and information loss at each stage of the process, allowing the data owner to make a decision on which set of operations better fits its privacy and utility needs. READ MORE.

SPANISH NATIONAL CYBERSECURITY INSTITUTE

Do guarantee the inviolable privacy of the human being

For children and educators: Read this blog article about the private information that kids and teens store on their mobile devices, including information security tips and guidelines for families to turn the device into a strongbox for their personal data. READ MORE.

At home: Our accounts are information safes which we must protect with strong passwords, creating copies and learning to identify attacks attempts. Information is power so, do you want to learn how to shield your accounts and protect your personal information?
READ MORE.

For SMEs: All you need to know to protect privacy and data security in your business also complying with GDPR. READ MORE.

SECURITY MADEIN.LU | Cybersecurity Agency for the Luxembourg Economy and Municipalities

Data protection and data privacy

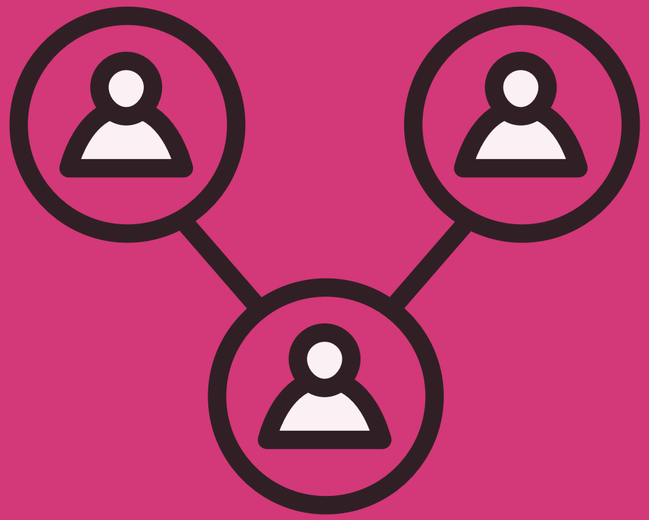
No matter what type of technological firewall we use, trust is indispensable in ensuring data privacy.

Like cybersecurity itself, data security and protection are multi-actor issues. Everyone involved has a responsibility: users need to consider how much they are sacrificing and sharing from their private sector, while those who process their data need to know what legislation they need to comply with. READ MORE.

SGS ISO/IEC 27701 Privacy Information Management Systems (PIMS) certification

ISO/IEC 27701 specifies the requirements and guidance for establishing, implementing, maintaining and continually improving a PIMS specific to your organisation. The standard is an extension of ISO/IEC 27001 (information security management) and ISO/IEC 27002 (security controls). It outlines PIMS-related requirements and guidance for personally identifiable information (PII) controllers and processors that are responsible and accountable for PII processing.

ISO/IEC 27701 can lead to: Greater trust in managing personal information, more transparency between key people, effective business agreements, defined roles and responsibilities, compliance with privacy regulations, and decreased complexity through integration with ISO/IEC 27001. An ISO/IEC 27701 audit from SGS will help you to stand out from the crowd by supporting you to develop and improve processes and increase skillful talent and sustainable customer relationships. In addition, SGS offers a range of complementary services across: Information security, Cloud, data privacy, and availability. READ MORE.



RESOURCES FROM THE COMMUNITY

The most common vulnerabilities found in APIs

Approach has published the Annual Pentest Report 2022 on APIs (Application Programming Interfaces) because their use is essential today, however they present their own vulnerabilities, listed in the 'OWASP Top 10 API vulnerabilities' on which we base our report.
The objective is to share identified vulnerabilities with the entire cybersecurity community. Approach's ethical hackers as well as DevSecOps engineers share tips and recommendations to improve the resilience and reduce the vulnerabilities of an organisation. READ MORE.

Data breach: The 5 worst consequences for the company

Companies often lack full awareness of the consequences associated with a data breach. A level of vagueness that leads to underestimating the risk and the need to prevent attacks. The truth is that an IT systems breach today can turn into a real disaster. READ MORE.

Nymiz helps you face the security and privacy challenge in sensitive data

AI-Based personal data anonymisation software: Nymiz detects personal data in unstructured files (doc, docx, xls, xlsx, jpg, tlf, png, pdf) and also in structured data (databases), and anonymises or pseudonymises them reversibly or irreversibly. In addition to mitigating data breach risk and avoiding privacy fines, Nymiz unlocks the value of data by allowing advanced analytics to be applied on masked data. READ MORE.

How to respond to a data breach under the GDPR

Many organisations are covered by the European Union's General Data Protection Regulation (GDPR), which not only regulates how companies should protect personal data, but also sets out what they have to do after experiencing a security breach involving personal data. Should the breach be reported to someone? Is it necessary to inform the affected person? If you want to learn more, read the article or download the infographic.

Technological essentials for privacy and data security

Securing company data is essential: GDPR rules and the (competitive) risks connected to data loss have moved this topic into the focus of strategic discussions. No matter if it is a cyber-attack, an employee’s mistake, or a failure of technology: secida's CEO Alpha Barry will share tips and tricks for securing company data in the best way possible by optimisation of IT infrastructure components, connected systems and processes. Join secida's Lunch&Learn on Wednesday, August 24th at 12pm CET (in German). READ MORE.

Syntho builds an AI generated synthetic data platform to boost data-driven solutions

As winner of the Philips Innovation Award, the Amsterdam based scale-up Syntho is on a mission to unlock privacy sensitive data to accelerate the adoption of valuable data-driven solutions with their AI generated synthetic data platform. This self-service platform is easy to use without prior knowledge required. Syntho supports complex data structures, such as multi-table databases, time series (longitudinal data) and huge databases with a “one click” approach. READ MORE.

THANK YOU

for your time!

The Cybersecurity Awareness Calendar
is an initiative launched by:
European Cyber Security Organisation (ECSO)
29, rue Ducale
1000 - Brussels

company/ecso-cyber-security

www.ecs-org.eu

@ecso_eu

secretariat@ecs-org.eu