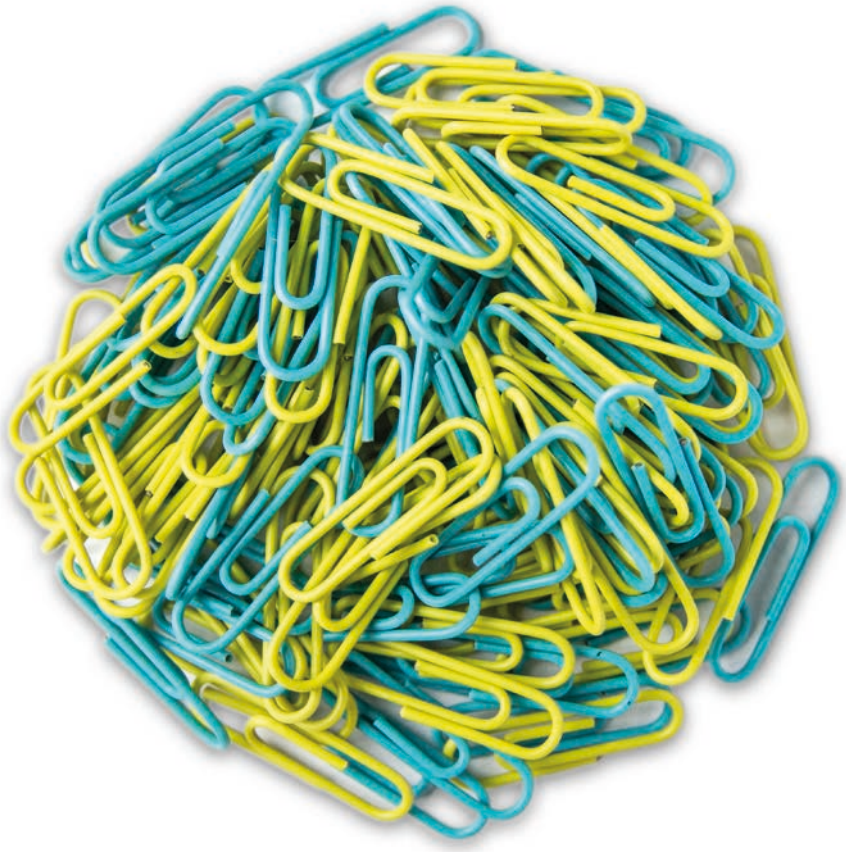
Deloitte.

SecurEnds



Supporting compliance with data protection regulations

Whitepaper on SecurEnds Credential Entitlement Management (CEM) solution

The General Data Protection Regulation (GDPR)

The GDPR[1] - i.e. the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th of April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. The GDPR came into effect on the 25th of May, 2018 and was designed by the European Parliament back in 2016 when the European Union recognized the importance of data protection for its citizens, especially as we see the changes that technology has made in our lives.

The GDPR has widened its reach by including international companies that collect data from any citizen in any EU Member State. This increase in reach will affect organizations founded within the EU, as well as organizations that are based in another country but offer their products and/or services to citizens of the EU. This means that if your business is located in a non-EU country such as the United States, Canada or Australia, and regardless of whether the GDPR legislation or its predecessor has ever had to concern you before, it will now. If a company is found to be non-compliant with the GDPR, the penalties include administrative fines that can reach either 20 million Euros (approximately 22 million USD) or 4% of the company's global annual turnover – whichever amount is greater.

Addressing GDPR compliance challenges by enforcing a strict control over user access to personal data stored in

In this context, companies that collect data from any citizen in any EU Member State have launched a variety of programmes and projects aimed at addressing the challenge of compliance with GDPR. One of the key challenges that companies encounter in their efforts for

According to GDPR, companies are encouraged to implement technical and organisational measures, at the earliest stages of the design of the processing operations, in such a way that safeguards privacy and data protection principles right from the start ('data protection by design'). By default, companies should ensure that personal data is processed with the highest privacy protection (for example only the data necessary should be processed, short storage period, limited accessibility) so that by default personal data isn't made accessible to an indefinite number of persons ('data protection by default').

Therefore, it is key for companies subject to GDPR to ensure an adequate control on the manner they manager the user access to their IT systems and platforms that store or process personal data. In particular, the 'data protection by default' principle must be complied with by ensuring a strong and regular control over users' entitlements for access across a very wide range of IT systems that store/process personal data.

Complying with GDPR Article 25 requires adopting and mix of both organizational and technology strategies and solutions.

A few organizational strategies are:

- Not copying production databases for development, testing, or analytics purposes. Instead the data should be anonymized or pseudonymized.
- Not storing spreadsheets and other data sources in a local folder or to a SaaS application such as Dropbox, Google Drive, or OneDrive.
- Limiting email archive access to a limited number of privileged users and monitoring their activity.
- Requiring encryption of emails containing identifiable personal data.
- Protecting personal data at-rest, in-motion, and in-use employing an existing database format.
- Setting and enforcing policies about using bring-your-own-devices to access secured data.
- Implementing staff training, internal audits of processing activities, policy reviews, and documentation of compliance

About SecurEnds Credential Entitlement Management (CEM)

The **SecurEnds Credential Entitlement Management (CEM)** product addresses user access reviews that grants enforce, revokes and administers fine-grained access entitlements (also referred to as "authorizations," "privileges," "access rights," "permissions" and/or "rules"). Its purpose is to review IT access policies to structured/unstructured data, devices and services from various endpoints including:

- Active Directory
- Windows Shared Folder
- Office 365 and Exchange
- SharePoint
- Unix/Linux
- Unix/Linux
- Database
- Network Access
- Oracle
- MySQL/Postgres
- VPN/Remote Access
- Google G Drive
- AWS/Azure cloud
- Salesforce
- SAP
- Jira
- GitHub
- Dropbox
- Box

SecurEnds Credential Entitlement Management (CEM)

product automates user access rights, access certification and remediation to meet security compliance for identity governance. It enables companies to continuously run review campaigns of the users' access rights and roles, assigning the manager to certify or revoke their entitlements, thereby increasing the security and accuracy of certifications and making the certification process auditable and compliant with a number of key legal and regulatory requirements, like for instance the compliance with GDPR key requirements.

[1] See https://eur-lex.europa.eu/eli/reg/2016/679/oj

About the Authors

Dan Cimpean
+32 497 59 38 27
dcimpean@deloitte.com
Gateway building, Luchthaven Brussel Nationaal 1 J
1930 Zaventem, Belgium
www.deloitte.be

Dan is a partner in Deloitte Consulting and Advisory, Belgium and is leading the cyber risk services offering towards the European institutions. He has over 17 years of experience in assisting EU bodies, national authorities and major industry actors on cyber security, regulatory compliance and risk management matters. Since 2008, Dan supports major European policy initiatives, including compliance with key laws and regulations, awareness and training, cyber capacity building and international cooperation.

Tippu Gagguturu
+1 678-374-4243
tippu.gagguturu@securends.com
1 Glenlake Parkway, Suite 525
Atlanta, GA 30328
www.securends.com

As a Co-Founder and CEO of SecurEnds, Tippu Gagguturu is responsible for growing SecurEnds, formulating and executing long-term strategies. Prior to co-founding SecurEnds, Tippu worked for Allconnect as Chief Information Officer and successfully led the IT team with a focus on the infrastructure, security, solutions, software, and delivery of technology platform for the Allconnect marketplace. Prior to joining the Allconnect, Tippu worked for Equifax, Fujitsu Consulting, and Tata Consultancy Services. In the past, Tippu has served as a consultant for clients such as Verizon, MCI, Merrill Lynch, Prudential Financial, and Walmart. Tippu received his Master of Technology from the Indian Institute of Technology (IIT) in Kharagpur, India.

Deloitte.

SecurEnds

SecurEnds is an information security company, offering a wide portfolio of security products including identity access management, identity provisioning/de-provisioning, employee on-boarding/off-boarding, identity governance, user access/ entitlement reviews, security compliance, and audits. We focus on securing identities in the organization to protect potential breaches, internal security threats, and meet security compliance and audits.

Deloitte.

Designed by CoRe Creative Services. RITM0338530