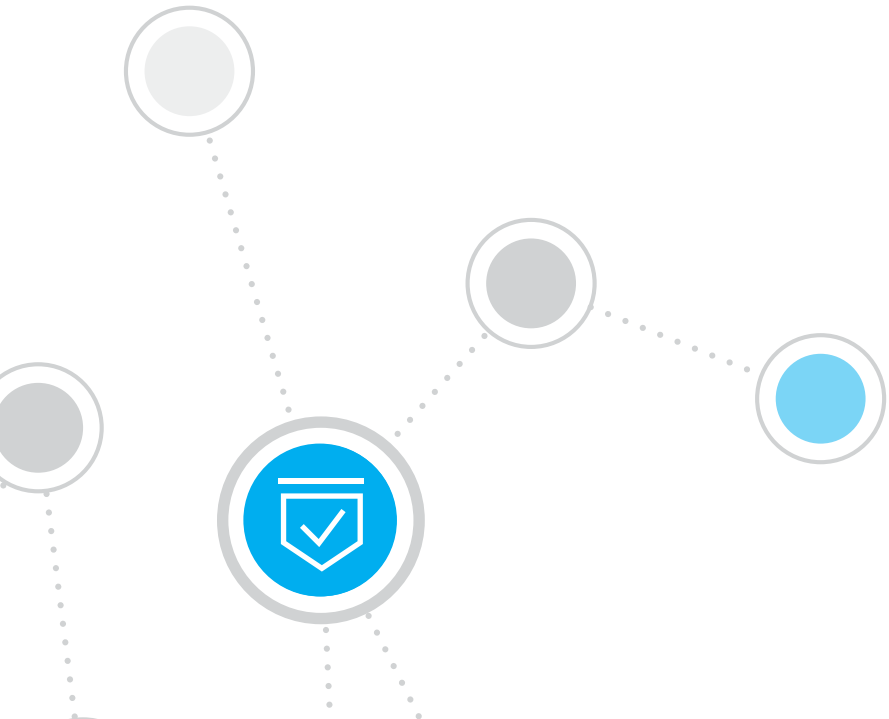
FORESCOUT

White Paper

GDPR: A Europe-Based Regulation with Global Impact



High-Profile Personal Data Security Breaches

- March 2017, Dun and Bradstreet: 33.6 million files.[9] This data contained names, email addresses and telephone numbers. Although this is information that Dun and Bradstreet notes would "typically be found on a business card," this data is included under the GDPR definition of personal data.
- May 2017, Google Gmail phishing attack,: potentially over a million users affected.[10] This highly sophisticated identity phishing attack led email recipients to an authentic-looking Google security page, which requested their consent to manage their email accounts, taking over their list of contacts.

Under GDPR, the "destruction, loss, alteration, unauthorized disclosure of, or access to" people's data must be reported to a country's data protection regulator within 72 hours after the organization identifies that there is a breach. The organization must then inform all data subjects impacted.[11]

1. What Is the GDPR?

On April 27, 2016, the European Union (EU) Parliament formally approved the General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679, which replaced the 20-year-old Directive 55/46/EC.[1] The new regulation is over 200 pages long and becomes effective on May 25, 2018.

GDPR applies to the processing of personal data or monitoring of EU residents ("data subjects") in the context of data controllers and data processors who do business in the EU or who provide services to EU residents, even if the business's base of operation is outside the EU (Article 3).[2] The focus is thus the data subject, not the location of the business. Personal data includes any information relating to an individual, whether it relates to his or her private, professional or public life, a name, a photo, an email address, bank details, posts on social networking websites, medical information or a computer IP.

2. What Purpose Does GDPR Serve?

GDPR is intended to protect the privacy and freedoms of EU residents by extending greater control and transparency of processing of their personal data through heightened regulations and the imposition of significant fines and penalties for violations of those protections (the greater of €20 million Euros or 4 percent of annual global turnover).[3] Furthermore, GDPR provides the added benefit of harmonizing the data privacy laws across the European Economic Area (EEA).

3. What GDPR Means to Companies

According to the GDPR principles set out in Article 5,[4] personal data must be:

(a) Processed lawfully, fairly and in a transparent manner

(b) Collected for specified, explicit and legitimate purposes

(c) Limited to what is necessary in relation to the purpose for which it is processed

(d) Accurate, relevant and kept up to date

(e) Kept and stored for no longer than necessary for the purpose it was processed and in accordance with appropriate technical and organizational measures

(f) Processed in a manner that ensures appropriate security that protects against unauthorized or unlawful processing, loss, destruction or damage

Companies need to consider two key factors: accountability and compliance. Under GDPR, companies will be more accountable for their handling of personal information. In fact, many organizations will need to:

- Change how they collect, use and transfer personal data
- Make changes to or implement new IT systems dedicated to maintaining appropriate technical and organizational measures with a level of security appropriate to the risk
- Update privacy notices, policies and contracts and terms with suppliers, customers, resellers and others
- Consider data privacy in product design by default, which may include pseudonymization and encryption of personal data

- Organizations must be able to notify the relevant supervisory authorities of a breach within 72 hours of discovery, including information on the breach, the measures taken to fix it and possible consequences[5]

4. What GDPR Means to Individuals

In addition to the accountability organizations now have in collecting and handling personal data, GDPR gives individuals much more power to access and control the information that is held about them:

- Organizations processing personal information must clearly explain that consent is being given and there has to be a "positive opt-in" from the individual. Controllers are also encouraged to develop interoperability among each other to make the subject's data portable and easy to move across the EU.
- Everyone has the right to get confirmation that an organization has information about them and to receive access to this information and any other supplementary information. Organizations must deliver the requested information within one month.
- GDPR also includes a person's rights regarding automated processing of data: individuals have the right not to be subject to a decision if it is automatic and if it produces a significant effect on a person.
- The new regulation also gives individuals the power to get their personal data erased in some circumstances: if it is no longer necessary for the purpose it was collected, if consent is withdrawn, if there's no legitimate interest and/or if it was unlawfully processed. Subjects must be able to withdraw consent with the same ease that he/she gave it.

5. What Security Professionals Should Know about GDPR

Although GDPR extends beyond traditional data security, it is the security aspect that causes organizations the biggest headaches, given the rapidly increasing number of data breaches. Below are relevant excerpts from the GDPR text. See footnote for references:

Article 25 "Data Protection by Design and by Default":[6]

1. *Taking into account the state of the art, the cost of implementation and the nature, scope, context and purpose of processing; organizations shall implement the appropriate technical and organization measures appropriate to the risk, including implement[ing] technical and operational measures such as pseudonymization and data minimization.*
2. *Implement technical and operational measures to ensure that only personal data which are necessary for each specific purpose of the processing are processed – involving the amount of personal data collected, the period of storage and their accessibility. In particular, measures shall be taken that default personal data are not made available to an infinite number of natural persons.*
3. *A certification mechanism shall be deployed to demonstrate compliance to paragraphs 1. and 2. above.*

Article 32 Security of processing[7]

1. *Taking into account the state of the art, the cost of implementation and the nature, scope, context and purpose of processing; organizations shall implement the appropriate technical and organization measures to ensure a level of security appropriate to the risk, including:*
    a. *the pseudonymization and encryption of personal data*
    b. *Ability to ensure confidentiality, integrity, availability and resilience of processing systems and services*
    c. *Ability to restore access to personal data in a timely manner in the event of a physical or technical incident*
    d. *Process for regularly testing, assessing and evaluating the effectiveness of the measures taken to ensure the security of processing*
2. *In assessing the appropriate level of security, specific account shall be taken to the risks caused by accidental or unlawful destruction, loss, unauthorized access to personal data.*

Article 33 "Notification of a Personal Data Breach to the Supervisory Authority":[8]

1. *In case of a personal data breach the organization shall inform the security authority without undue delay and, where feasible, not later than 72 hours after they have become aware of it.*
3. *The notification shall at least:*
    a. *Describe the nature of the personal breach and approximate number of data subjects and personal records concerned*
    b. *Communicate name and contact details of the Data Protection Officer, if applicable*
    c. *Describe the likely consequences*
    d. *Describe the measures taken to address the personal data breach and/or measures to mitigate the possible effects*

6. Transforming Security Through Visibility

GDPR privacy protection principles and obligations, covered by the articles above, may have far-reaching consequences.

As a first step to becoming GDPR-ready, companies need visibility into what is on the network. They need to know which devices are connected to the network, who is using these devices, the access rights they have, when they are connected and which data they are allowed to access. Organizations need proof that mechanisms on these devices to secure private data, such as encryption agents, are operational.

Visibility in this case is not limited to just corporate-managed devices but also includes a plethora of different bring your own device (BYOD) and Internet of Things (IoT) computers or other devices that may be used as part of the organization's primary process, or devices that are used by employees but need to be blocked from accessing personal data.

Given the huge proliferation of devices, organizations need a different approach, as the traditional agent-based security solutions do not provide a complete solution. Instead, organizations need to work in an agentless manner to see and manage all these different devices.

Recommended Steps for IT Security Personnel

1. Based on the information collected on the device and user, IT personnel can take control measures to help ensure devices, applications and users are working in accordance with both GDPR and the company's security policies.
2. To help ensure that the organization maintains security of processing—and, more importantly, minimizes the risk caused by accidental or unlawful destruction, loss and/or unauthorized access to personal data—network segmentation is essential. Network segmentation is not new, but it has become harder to deploy, resulting in organizations choosing ease of use over security.
3. Applying the appropriate controls in a manual way is a losing proposition. It is too costly and does not provide the necessary guarantees. Companies need automated policies to enforce their security operational processes—and, via automatically generated reports, demonstrate compliance to the security authority.
4. Identifying a security breach in today's world can be a complex activity, potentially involving many security solutions. Orchestration, the sharing of information between different security appliances, allows you to share disparate information across these solutions, which is key to quickly identifying a security breach.

7. Conclusion

Every company that holds and processes the data of European citizens is required to comply with the new EU GDPR, no matter where they are located in the world. Being noncompliant with this regulation can be very costly—up to 20 million Euros or up to 4 percent of a company's annual turnover.

Accountability and compliance are two key words linked to GDPR. Companies need to demonstrate within reason that they implemented the appropriate technical and operational measures to secure and protect personal data. For definitions, see the official GDPR text in links below. For more information on how ForeScout can help you gain visibility, see the "Learn More" section below.

Learn More

How ForeScout Technologies Inc. is Preparing for GDPR Case Study

Addressing the EU General Data Protection Regulation (GDPR) Solution Brief

ForeScout Extended Modules for SIEM Solution Brief

EU GDPR home page

[1] EU GDPR.org Website: https://www.eugdpr.org/gdpr-timeline.html
[2-5] Official GDPR Text (PDF): http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf
[6] See Article 25: https://gdpr-info.eu/art-25gdpr/
[7] See Article 32: https://gdpr-info.eu/art-32gdpr/
[8] See Article 33: https://gdpr-info.eu/art-33gdpr/
[9] Dun & Bradstreet database breached, 33.6M files vulnerable. https://www.scmagazine.com/dun-bradstreet-database-breached-336m-files-vulnerable/article/644419/
[10] Massive Phishing Attack Targets Gmail Users https://www.nbcnews.com/tech/security/massive-phishing-attack-targets-millions-gmail-users-n75450
[11] See Article 33: https://gdpr-info.eu/art-33gdpr/

Learn more at
www.ForeScout.com

FORESCOUT

ForeScout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591

ForeScout Technologies is transforming security through visibility, providing Global 2000 enterprises and government agencies with agentless visibility and control of traditional and IoT devices the instant they connect to the network. Our technology continuously assesses, remediates and monitors devices and works with disparate security tools to help accelerate incident response, break down silos, automate workflows and optimize existing investments. As of December 31, 2017, more than 2,700 customers in over 80 countries improve their network security and compliance posture with ForeScout solutions. See devices. Control them. Orchestrate system-wide threat response. Learn how at www.forescout.com.