BTB SECURITY

DATA PRIVACY IN THE EUROPEAN UNION

BECOMING COMPLIANT WITH NEW PROTECTION MEASURES

The General Data Protection Regulation 2016/679 (GDPR) is an action passed by the European Parliament, Council of the European Union (EU), and European Commission to unify and strengthen data protection for all individuals and return control of personal data to citizens. The action also unifies regulations among EU member states, simplifies the regulatory environment for international businesses, and addresses the export of personal data outside the EU.

Enforceable on May 25, 2018, GDPR replaces Directive 95/46/EC 2 of 1995. It does not require enabling legislation through the governments of individual member nations—making it directly binding and applicable. Further, the GDPR extends the concept of personal data to include any data element that may identify, directly or indirectly, the "Data Subject." This includes a name, a photo, an email address, bank details, social network posts, medical information, or a computer IP address.

With controversial topics surrounding this regulation, much conversation will surely take place. For example, technology firms and industries who have long had data-retention requirements may find data destruction—the Right to be Forgotten detailed below—difficult to integrate. They will likely need to change both their processes and use of technology.

Just as with the adoption of the Health Insurance Portability and Accountability Act (HIPAA)—a similar data-protection regulation—there are organizations that will be slow to react to these changes. Enterprise organizations are most likely to take these requirements seriously—and act upon them quickly. Highly regulated industries—such as finance, healthcare, and others where compliance requirements and formalized information security programs are commonplace—will likely be the quickest to adapt.

KEY DATES

OCTOBER 24, 1995
The EU created Data Protection Directive 95/46/EC to regulate processing personal data.

JANUARY 25, 2012
The European Commission submitted a proposal for updated data protection regulations.

DECEMBER 15, 2015
The Parliament and Council agreed on the text of an agreement to finalize and sign.

APRIL 8, 2016
The Council of the European Union formally adopted the text of the agreement as written.

APRIL 16, 2016
The European Parliament formally adopted the text of the agreement as written.

MAY 25, 2018
The GDPR becomes fully enforceable throughout the EU after a two-year grace period.

GUIDING PRINCIPLES

Both the GDPR and the original Directive 95/46/EC are based on even older principles established to protect personal data and the right to privacy. When the Organization for Economic Co-operation and Development (OECD) originally adopted a set of recommendations in 1980, it set forth eight guiding principles for the processing of personal data.

THESE INCLUDE:

COLLECTION LIMITATION
There should be limits to the collection of personal data, data should be obtained by lawful and fair means and—where appropriate—with the knowledge or consent of the data subject.

DATA QUALITY
Personal data should be relevant to the purposes for which they are to be used and—to the extent necessary for those purposes—should be accurate, complete, and up-to-date.

PURPOSE SPECIFICATION
The purpose for collection of data should be specified at the time of collection and data should not be used for anything other than its original intention without notifying the subject.

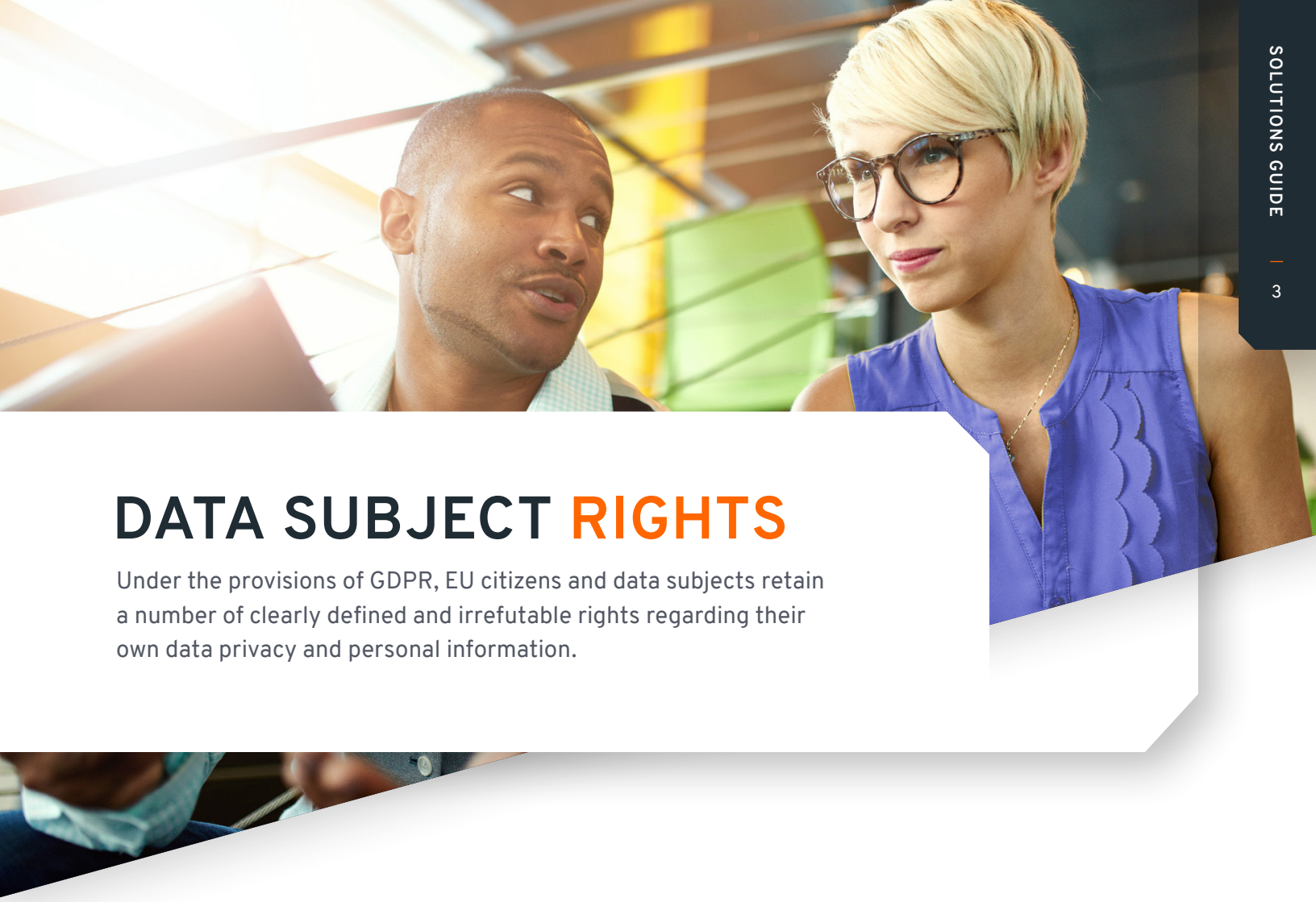
USE LIMITATION
Personal data should not be used for purposes outside of the original intended and specified purpose—except with the consent of the data subject or the authority of the law.

SECURITY SAFEGUARDS
Personal data should be protected by reasonable security safeguards against risks such as loss, unauthorized access, destruction, use, modification, or disclosure.

OPENNESS
There should be a general policy of openness about developments, practices, and policies—and individuals should have easy access to information about their personal data—including who is holding it, and for what use.

INDIVIDUAL PARTICIPATION
Individuals have the right to know if a controller has data and access that data in an intelligible form for a reasonable charge—and can challenge a controller for refusing to grant access or challenging data accuracy.

ACCOUNTABILITY
Data controllers should be accountable for complying with the measures detailed above.



DATA SUBJECT RIGHTS

Under the provisions of GDPR, EU citizens and data subjects retain a number of clearly defined and irrefutable rights regarding their own data privacy and personal information.

THESE INCLUDE:

CONSENT
Companies must explicitly request consent in a clear, intelligible, and easily accessible form using plain language. At the same time, it must be just as easy for a data subject to withdraw consent as it was for them to initially give it.

BREACH NOTIFICATION
Notification within 72 hours is now mandatory in instances where a data breach may risk the rights and freedoms of individuals. Data processors must notify customers and controllers without delay once aware of a breach.

RIGHT TO ACCESS
Data subjects can obtain from controllers confirmation their personal data is being processed—including where and for what purpose. Data controllers must also provide personal data free-of-charge in an electronic format.

RIGHT TO BE FORGOTTEN
Data subjects can have controllers erase personal data, cease further dissemination of data, and have third parties halt processing of data when such data is no longer relevant or when a data subjects withdraws consent.

DATA PORTABILITY
Under the GDPR, data subjects have the right to receive personal data that they have previously provided in a commonly used, machine-readable format. They also retain the right to transmit that data to another controller.

PRIVACY BY DESIGN
From the onset of system design, controllers can hold and process only the personal data absolutely necessary to complete their duties. GDPR also limits access to personal data to those who require it for processing.

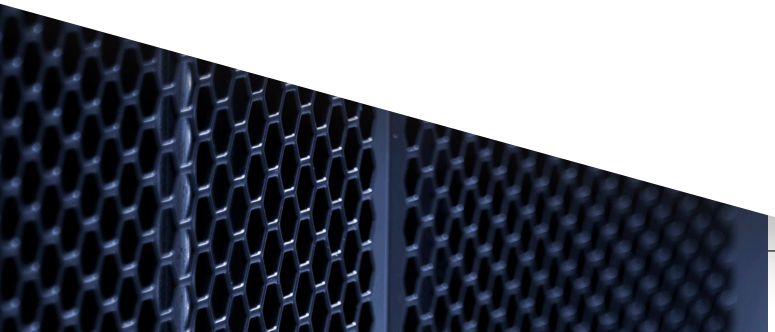
WHO DOES THE GDPR EFFECT?

The reach of the GDPR extends far beyond the EU member states, and applies to any organization that offers goods or services to or monitors the behavior of EU citizens or data subjects. The regulation applies to all companies that process or hold the personal data of EU citizens or data subjects regardless of the company's physical location. And when coupled with the broad definition of "personal data," the GDPR introduces new challenges to organizations operating internationally. While large enterprise organizations often have the resources to throw at GDPR compliance, smaller or mid-size businesses will likely encounter the greatest pains. These organizations may not have the necessary capabilities—or know specifically where they are to direct them.

DATA PROTECTION OFFICERS & ACTS

Under existing regulations, data controllers must notify the Data Protection Authority of their member state. The different notification requirements of EU member states mean that this reporting requirement can prove very difficult for multinational organizations. With the GDPR in effect, submitting notifications or registrations of data-processing activities to each member state's DPA will no longer be necessary. In addition, organizations will no longer need to notify DPAs or obtain approval for transfers as currently required under Model Contract Clauses (MCCs). Rather, internal record keeping will supplant these requirements. The appointment of a Data Protection Officer (DPO) will only be mandatory for controllers and processors that require regular, systematic, large-scale monitoring—including those who process data related to criminal records.

> The regulation applies to all companies that process or hold the personal data of EU citizens or data subjects regardless of the company's physical location."



PENALTIES FOR NON-COMPLIANCE

The penalties in place with the GDPR are very real. After the enforcement date of May 25, 2018—organizations not in compliance with the GDPR will face heavy fines. The penalties for non-compliance or a breach of GDPR include tiered fines of 2% for not keeping records in order, failing to conduct an impact assessment, or failing to notify authorities or data subjects in the event of a breach—up to 4% of the organization's annual global turnover. The EU can impose a maximum fine of €20 Million for the most-serious infringements. These include insufficient consent to process customer data or violation of core of privacy concepts. These fines can apply to both controllers—entities that determine the purpose, conditions, and means of processing data— and processors—entities that process personal data on behalf of controllers. This extends to the cloud, as well.

THE KEY TAKEAWAY

In a data-sensitive world, the GDPR aims to protect citizens from data and privacy breaches. The most important thing to remember is to be proactive. Get ahead of the issue. Though enforcement is months away; the sooner an organization moves toward compliance, the better off they will be.

There is no packaged solution an organization can buy that will bring them into compliance. Many try to purchase a "widget" that will bring them security—but they are never successful. Partnering with professional security consultants who understand both the risks and the stakes is an important first step. Those organizations that already partner with security professionals and have the appropriate framework and formalized programs in place are traditionally better suited to face any emerging regulatory changes and the potential security issues that follow.

> Those organizations that already partner with security professionals and have the appropriate framework and formalized programs in place are traditionally better suited to face any emerging regulatory changes..."

ABOUT THE AUTHOR

Matthew Wilson is an Information Security Advisor at BTB Security, a specialized cyber security services firm that specializes in proactively detecting threats as well as defending against and defeating cyber security adversaries. His background in network security, penetration testing, and assessment helps organizations shield their assets, customers, and employees against security breaches.

MATTHEW WILSON
(CISSP, GPEN, GSEC)

WHAT WE DO

BTB Security helps organizations worldwide detect, defend and defeat security breaches. From ethical hacking and vulnerability assessments to comprehensive managed security services programs, incident response and forensic analysis, BTB's solutions are designed to provide comprehensive security to organizations of all sizes.

BTB SECURITY