How Does Blancco Help Organizations Comply with the EU General Data Protection Regulation?

On May 25, 2018, the EU General Data Protection Regulation (GDPR) came into effect throughout Europe, and any global business that handles information from EU citizens and residents must prove compliance.

One significant update in this regulation is the expanded definition of personal data. Understanding what constitutes personal data is key to defining the scope of the data being handled by an organization.

Personal Data is defined information that relates to a natural person; the person is identified or made identifiable, directly or indirectly, by reference to an entity such as a name, ID number, location data or other unique identifier.

Once you understand what personal data is, it's important to then recognize what is meant by data processing and who oversees this responsibility.

GDPR Terminology:

Controller – the entity (person or organization) that determines the purposes and means of the processing of personal data.

Processor – the entity that processes personal data on behalf of the controller.

Processing – any operation performed on any piece of personal data, automated or not, including (but not limited to) collection, recording, organization, structuring, storage, retrieval, transmission, dissemination and erasure or destruction.

It should be noted that when a controller selects a processor to process data, he/she must agree to a binding contract ensuring that the same level of data protection is offered as stipulated by the regulation. This in effect means that the controller will not bear the full brunt of sanctions (previously the case), should a processor be liable for breaking the law.

The Right to Data Erasure

The right to erasure (also referred to as the 'right to be forgotten') extends the long-standing requirement that the Data Protection Directive contains—the right consumers have to request that their data or physical information be disposed of effectively and responsibly. The GDPR expands this right (and supersedes the Directive) to include data that lives on the internet. Consumers can request that they can "be forgotten" from the public view in specific circumstances.

The Right to Erasure Applies When:

- An individual withdraws consent
- An individual objects to the processing, and there is no overriding legitimate interest for continuing the processing
- An individual's personal data was unlawfully processed
- An individual's personal data is processed in relation to the offer of information security services to a minor

Under the existing Data Protection Directive, the right to erasure is limited to processing that causes substantial and unwarranted distress or damage. This is not true under the GDPR; however, if such distress or damage is in place, the case for erasure will likely be that much stronger. There are some specific instances in which the right to erasure does not apply, and organizations can refuse to deal with a request.

Organizations Can Refuse to Comply with a Request for Erasure When Personal Data is Processed for the Following Reasons:

- The exercise or defense of legal claims
- For public health reasons in the public interest
- Archiving purposes in the public interest, including statistical purposes, scientific research or historical research
- To exercise the right of freedom of expression and information
- To comply with a legal obligation for an exercise of official authority or performance of a public interest task

Data Minimization

While the 'right to be forgotten' has received a lot of media attention, the EU GDPR also includes important data minimization requirements that are dangerous if overlooked. Data minimization is defined as the practice of limiting personal data collected to the bare minimum required for its original purpose. This is expressly stated in Article 5(1)(c): "The personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimi[z]ation')."

What does this mean? It's important to start with looking at data minimization from a higher level. For example, if a website requests a user's phone number when completing a purchase, IT departments must pinpoint what systems this number is transferred to and which business requirements this personal information satisfies (to both determine if the data is actually necessary, and if it is, to have documentation of this reason in the case of an audit).

Data controllers (individuals, groups of individuals or organizations that determine the purposes for which, and the manner in which, any personal data is or will be processed), are responsible for justifying why each piece of personal data is collected and when it should be securely erased. Such an idea has been elucidated succinctly by the Privacy by Design approach: "minimize collection of personal data; delete personal data that's no longer necessary; restrict access and secure data throughout its entire lifecycle."

How Blancco Data Eraser Solutions Can Help

If you find yourself doing a gap analysis on your org's GDPR compliance and you find that personal data is sitting in your infrastructure or network and must be addressed, it's time to employ a data erasure solution to help. Software-based data erasure is the best way to achieve data erasure across your organization's full suite of IT assets. As ICO Commissioner Elizabeth Denham stated in her January 2017 speech on the GDPR, "Having the right mindset towards data protection helps to future proof a business. It will put it in the right place to keep up with legislation." Ensuring that data that is outdated, unnecessary or has been requested for removal is securely erased is as important part of future-proofing your organization's security posture.

Examples of How Blancco Can Help

Blancco File Eraser

If you have identified personally identifiable information (PII) on the file level (e.g. a copy of a customer database or a file structure with individual files and folders), Blancco File can target and erase files on computers and servers. The solution is available on both UNIX and Windows operating systems.

Blancco Drive Eraser

When you are re-deploying or decommissioning entire drive-based systems containing personal data, Blancco Drive Eraser increases endpoint security by erasing all data securely on enterprise laptops and desktops, as well as servers, storage systems and loose drives.

Blancco Mobile Diagnostics & Erasure

Once you have identified personally identifiable information on mobile devices or tablets, Blancco Mobile Diagnostics & Erasure can target and erase data on any device that's iOS or Android-based, using factory reset or other more advanced erasure methods.

blancco

Blancco LUN/ Virtual Machine Eraser

If you have stored PII temporarily on virtual volumes or in virtual machines, on-premise or in the cloud, Blancco Virtual Machine Eraser and/or Blancco LUN Eraser can securely target erase this data.

Blancco Management Console

For each of these erasure scenarios (and for every erasure performed), Blancco erasure solutions create a detailed audit trail to help prove compliance with regulations such as the GDPR. With Blancco Management Console, your organization will benefit from a centralized point of data management for these reports, along with the ability to manage all data erasure licenses, create and modify users and have complete visibility of their erasure activities—even across multiple locations. This will strongly contribute in your journey towards full GDPR compliance.

Why Blancco?

For 20 years, Blancco has offered solutions that support compliance with data protection and privacy regulations such as the new General Data Protection Regulation (EU GDPR). We support the need for heavily-regulated industries to stay compliant with these regulations with data erasure solutions that satisfy (and often exceed) those requirements.

Click here to learn more about how Blancco helps organizations meet data erasure requirements across the globe.