

EDPB Guide 2024

Wednesday 17 January 2024

**Guidelines 2/2023 on Technical Scope of Art.5(3) of
ePrivacy Directive**

Executive Summary

The importance of developing strategies around the ePrivacy Directive Technical Scope of Art, is to develop such strategies around implementing solutions through the use of the data, hardware equipment and the use of these devices within a data communication network.

The overall guide has discussed important details through the use of data and how it is scoped out through the equipment which it is deployed on.

A set of guidelines, has been developed to ensure the effectiveness of data usage and storage within corporations and through individual use.

The immenseness of such documentation is to create a secure way of dealing with the data both external and internal. Given the fact that the increase of Cyber Attacks on a global scale has caused major disruption through the data communication network.

Therefore the need to address solutions around a global phenomenon is to allow companies to strategise solutions around such issue, where data is dealt securely both internal and external within corporations.

It is indeed ever important to understand as what is deemed useful data when used on storage devices and data communication networks, so it ensures the safety of data collection through corporations.

Recreating systems and controllers

Data has increased since 2023, that there is a need to understand as how to create secure and safe measures around data usage and storage within corporations.

2024 has seen an increase in Cyber Attacks and the need to understand as how the data is used and stored within corporations is indeed an important safety measure around data security and storage.

The aim to address such issue is to develop methodologies around data and the importance of how it is used and stored.

There were certain sections of the guideline which needed clarification on as how to develop methodologies around such topic.

3.1 URL and Pixel tracking, Paragraph 47

“ Tracking pixels on websites link to an entity aggregating many such requests and thus being able to track users' behaviour.”

This section requires a bit more clarification around as how tracking pixels through a website is going to improve the users experience around website browsing. The downside when using such technique as tracking, as it goes against the ownership of data as how corporations track users behaviour and the type of data that is collected to allow a website to do so.

The way to view such issue is that website owners would have quite an advantage over such technique as it allows the use of tracking without the end users knowing as what occurs behind the scenes.

The most important way to address such issue is that the need to implement tracking measures does improve websites in terms of quality and detection. Yet when the end users are not quite aware of this occurring, then it goes against the data rights of the end user.

Therefore it is important to develop such measure which covers the use of tracking to a certain extent, else it invades the privacy of end users.

When such technique is used then it does allow website owners to view the data through external and internal networks.

Therefore tracking users behaviour is something to reconsider as how to address this, as the increase in cyber attackers is only going to allow the attackers to use this as their strategy to increase data collection within their end.

It is important to safeguard such measure to balance out as how much tracking is needed as opposed as to how much tracking goes ahead even when the ends users are not aware of it.

Implementing safety measures which doesn't allow outside attackers through internal and external networks is important as with the increase in cyber attacks, it is important to prevent such attacks from occurring from the very start. Therefore the aim is to create system controls that reduces the attacks or even improve the tracking of users behaviour is a way to view the issue both internally and externally within corporations. Cyber attackers would use tracking as a way to collect data to improve their attack and also create fortune from it. It is ideal to catch out these attackers even nearing a solution to combat the cyber attacks. Therefore everything starts with data and the system controls of how the data is stored is to ensure cyber attackers don't quite get their hands on sensitive information.

The overall guide which covers the eDirective Privacy Technical Scope of Art covers important information as how to use and store data within data communication networks and hardware equipment within corporations.

The need to safeguard and implement important system controls allows corporations to secure their network environment and to prevent cyber attackers from attacking both internally and externally.

Addressing the issues is another way of creating a safe environment for both corporations and the end users. within a data communications network

ICCYSS

Jefferson Tukimata