Europe Data Protection Board Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR Version 1.0

Thursday 31 October 2024

Executive Summary

The Europe Data Protection Guide evaluates a complete summary of how personal data is used both internal and external within corporations.

The importance of these guidelines is to emphasise how areas of work in which data is dealt with, coincides with both a practical and technical sense, when implementing solutions that safeguards both employers and employees within corporations.

Evaluating such guide is of great importance, as how to view personal data is used within corporations. The increase of technology such as A.I, has created such a debate as how to work around a vast amount of data especially synthetic data.

Despite the implementation of A.I technology, there still needs a coherent and robust method of implementing solutions around both data controllers and data subjects, that highlight the need of addressing key areas that focus within creating a secure environment both internal and external as how data is used, stored and implemented.

Introduction

The Europe Data Protection Guide covers information which establishes the importance of how data is used within corporations, and how the guide is used to implement solutions around the use of personal data. Section 2.2, Clause 46 would need amending as what is deemed continuous observing both from the data subject and also the data controller.

2.2. The context of the processing

46. In addition to adverse outcomes that can be specifically foreseen, 55 the controller may need to take into account also possible broader emotional impacts resulting from a data subject losing control over personal information, or realising that it has been misused or compromised. The chilling effect on protected behaviour, such as freedom of research or freedom of expression, that may result from continuous monitoring/tracking or from the risk of being identified, should also be given due consideration. For example, continuous online monitoring of online activities by a platform may give rise to the feeling that a data subject's private life is being continuously observed

Strategy:

Clause 46 would still need a bit of clarification as what is meant by the data subject's private life, continuously observed. The need to address this clause is still unclear. The term 'Observed' which is constantly monitoring 24/7 which includes tracking a data subject without their permission. What information would need addressing within the Privacy Act that covers security within both ends. Would the Privacy Commision within each country have to update their Documentations to clarify this section to ensure security is covered within both internal and external. If so how much tracking would a data controller have till it invades the privacy of the data subject?

So what needs a bit clarification is, would the data subject still go through constant observeration or tracking even when using a cellphone to access online activity. A note that needs to be taken, does 'tracking' even fall into this category. Does another section need to be covered that discuss the level of tracking where it is appropriate. How much control does a data subject have, till they know that are tracked. If so, it is important to take note what corporations can undertake, and to what degree the data subject has as oppose to the data controller. Would a random neighbour that continuously observes a data subject or even tracking, deemed a breach of confidentiality. If so then it is important to take note as what data would entail them into doing such thing with out permission. What degree would the observer that does this illegally, have to go through till the data subjects private life is exposed. Ensuring that this clause is clarified is going to bring a sense of security within the data subject and also the data controller. The clause would also affect as how the humanitarian act plays an important role to freedom of speech within the data subject and the data controller. It is something to take note of when re-creating the clause which caters to both parties, so it ensures that personal data is used a coherent way while maintaining the security both internal and external within corporations.

Personal data use is also compromised even when spies within countries and even undercover agencies that undertake their work which exposes the vulnerabilities of the data subject without them even knowing. To what extent would such tasks reduce that would disallow spies or even undercover enforcement agencies within countries would have to go through to ensure that doing such task is a breach of the data subject's confidentiality. In order to walk in a safe, secure environment, especially corporations, it is ever so important that spies that track without consent or

even undercover agencies that do such task would need a valid reason as why they would perform such task around a data subject within every country around the world. Doing so allows the data subject to undertake tasks without the data subject feeling as someone or something is watching their every move. Enforcement industries is a area where a great amount of data is used. When the data subject goes through such tracking without a valid reason, to what extent does the data subject have the right to report such matter while maintaining their actions through the humanitarian act. Do enforcement industries that track data subjects without permission have to receive a infringement of some sort that entails as what would allow them to do such task illegally. A area which the guide would need to cover in order to safeguard both the actions of the data subject and data controller when spies and undercover agencies are involved in such task.

A.I technology has also increased as how personal data is used. A.I equipment can even define areas a data subject goes through even without the data subject saying anything. Does A.I equipment have a hidden tracking device or even a hidden camera that compromises the data subjects exposure of their private life. Is there a way around reducing such tracking or even embedding or even informing a data subject as how their personal data is used within A.I equipment such as A.I televisons? When data is used through A.I equipment and is exposed without the data subject knowing, then it is important that the data subject is aware as how to ensure employees are safe within corporations, whether it's through documentation or even external partnerships with corporations.

Drones is a area where personal data would need addressing, as drones could still access personal data without the data subject knowing. How would corporations including countries reduce the use of drones through a external attack amongst data subjects. Everything that drones go through is controlled through the data controller. Is there a way to reduce or even eliminate drones used within environments especially external attacks amongst civilians. Drones is a equipment which defines the data subject including the data controller when personal data is used. A drone which captures personal data of the data subject while going against the data ethical use and humantarian act when using such technology, is deemed inappropriate use of the technology. There is a need to address such scenario as soon as possible in order to reduce or even eliminate the use of drones within a combat environment. Doing so would disallow countries using drones for inappropriate use especially combat situations.

The guide entails important information that discuss the import uses of personal data. Within a world where A.I technology has increased it's uses within corporations, it is important that the use of synthetic data and how it is used, covers methodologies that allow corporations to provide solutions as how to work around and create strategies that allow both the data controller and data subject techniques in safeguarding personal data especially A.I Technology.

Jefferson Tukimata