**Data Protection in Humanitarian International Organisations: Balancing Operational Needs and Privacy Standards**

*This study, conducted as part of an LL.M in Privacy, Cybersecurity, and Data Management, was partly funded by the Tertiary Education Scholarship Scheme of Malta. It explores a critical issue facing humanitarian international organisations: how to balance operational efficiency with stringent data protection standards, particularly in the context of the European Union’s General Data Protection Regulation (GDPR).*

In today’s interconnected world, international humanitarian organisations face a growing challenge: balancing operational effectiveness with the stringent privacy standards set by the GDPR. These organisations, from the International Committee of the Red Cross (ICRC) to the United Nations High Commissioner for Refugees (UNHCR), are at the forefront of disaster relief, conflict resolution, and humanitarian aid. Yet, the digital age has introduced new complexities to their missions, particularly in managing sensitive personal data. Humanitarian international organisations (IOs) collect, process, and share personal data to deliver critical aid. This data ranges from health records and biometric identifiers to contact information for refugees and displaced persons. Although essential for operations, such data processing involves inherent risks, especially in contexts where the populations are vulnerable and where cybersecurity infrastructure may be inadequate. At the heart of this dilemma lies the GDPR, which has raised the bar for data protection worldwide. While the regulation’s primary focus is on protecting the personal data of individuals within the European Economic Area (EEA), its implications are felt far beyond Europe’s borders. Humanitarian IOs, however, operate under a unique legal framework that grants them privileges and immunities, effectively exempting them from national laws, including the GDPR. This creates significant challenges for organisations that need to exchange data with European entities bound by GDPR obligations.

**Operational Complexities and Legal Immunities**

Humanitarian organisations rely on data to save lives and deliver aid efficiently. For example, tracking the movements of displaced populations or monitoring the health conditions of refugees requires the secure handling of sensitive information. Yet, IOs often work in regions plagued by instability, where data security measures can be hard to implement. In 2022, the ICRC suffered a cyberattack that exposed the personal data of over 515,000 vulnerable individuals, demonstrating the critical importance of strong data protection measures. Despite the vital role they play in crisis management, humanitarian IOs often find themselves caught between their operational needs and the legal requirements imposed on data by the GDPR. One of the central issues is the reliance on derogations—temporary exceptions that allow data transfers when no permanent legal framework exists. These derogations are meant to be used sparingly but have become the default for many IOs because no long-term solutions have been established. This reliance contradicts GDPR guidelines, which state that derogations should not be the rule for international data transfers.

**The Search for Sustainable Solutions**

One potential solution identified in the thesis is the pursuit of Adequacy Decisions by the European Commission, which would formally recognise that an international organisation provides a level of data protection equivalent to that of the GDPR. However, no humanitarian IO has sought such a decision, largely because it would require significant changes to their operational structures and legal immunities. Another promising approach is the adoption of Binding Corporate Rules (BCRs). These rules, typically used by multinational corporations, could be adapted to the unique context of IOs. BCRs would allow organisations to maintain consistent data protection standards across their operations while respecting the legal exemptions that enable them to function independently. Tailoring BCRs to fit the specific needs of IOs would require careful negotiation and adaptation but could provide a more permanent framework for managing data transfers.

**Recommendations for Enhanced Data Protection**

The thesis also emphasises several key strategies to enhance data protection within humanitarian international organisations. One crucial approach is the implementation of regular training programs. These training sessions should be scenario-based, ensuring that staff, particularly those operating in emergency situations, are fully equipped to handle sensitive data in compliance with GDPR standards. These programs must be ongoing, given the dynamic nature of humanitarian work, and should emphasise the practical application of data protection principles in high-pressure environments.

Another important recommendation is the development of comprehensive data protection policies tailored to the specific operational challenges faced by humanitarian organisations. These policies must focus on data minimisation, ensuring that only essential personal data is collected. Clear protocols should be established for how data is shared with other entities, including local governments and non-governmental organisations, and robust procedures should be put in place for managing data breaches. Additionally, the use of Data Protection Impact Assessments (DPIAs) is advocated as a key tool for evaluating the risks associated with new data processing activities. DPIAs should be conducted at the outset of new projects and whenever there are significant changes to existing processes. This proactive approach will help humanitarian organisations align their operations with GDPR standards while addressing potential privacy risks early in the project lifecycle.

The thesis also highlights the importance of investing in advanced technological safeguards, such as secure data storage and encryption tools, to protect sensitive information in the field. In environments where infrastructure is often compromised, these technological measures can play a critical role in ensuring that personal data remains secure during transfer and processing.