THE DECLARATION PRINCIPLES

THE SIGNATORIES SUPPORT THE FOLLOWING FUNDAMENTAL PRINCIPLES:

- **A stakeholder-centered approach**: Adopting a stakeholder-centric approach to cybercrime reporting, where the needs and perspectives of SMEs, industries, associations, LEAs, and CERTs are given priority. A stakeholder-centered approach is important because it prioritises the needs and perspectives of all stakeholders involved in the project. This approach takes into account the impact of the project on each stakeholder group and works towards creating solutions that benefit all parties. This helps to ensure that the project is more inclusive and sustainable, as it addresses the diverse needs of stakeholders and creates buy-in and support for the initiative. Additionally, a stakeholder-centered approach helps to build trust and foster collaboration among the stakeholders, which can lead to more effective and efficient solutions.

- **An EU-wide cooperation and collaboration approach**: Encouraging cooperation and collaboration among all stakeholders to increase reporting of cybercrime in the EU and enhance the overall security of the online world. An EU-wide cooperation and collaboration approach allows for a more comprehensive and coordinated effort to address issues and achieve common goals. By working together, stakeholders from different countries and regions can share resources, knowledge, and expertise, and leverage the strengths of each other to overcome common challenges. This can lead to more efficient and effective solutions, as well as greater impact and benefits for society as a whole. Additionally, an EU-wide cooperation and collaboration approach can help to address the digital divide and reduce inequalities across the EU, ensuring that all citizens have equal access to the opportunities and benefits of technology.

- **A data-driven and open innovation ecosystem**: Encouraging the sharing of information and best practices to promote the development of a common approach to cybersecurity and reduce the impact of cybercrime on society. An EU-wide data-driven and open innovation ecosystem allows for the sharing of information and best practices, which in turn promotes the development of a common approach to cybersecurity. This helps to reduce the impact of cybercrime on society, as a collective effort is made to prevent and mitigate cyber threats. By encouraging the sharing of data, the ecosystem creates a culture of collaboration and transparency that allows for a more effective and efficient response to cybersecurity challenges. Furthermore, an open innovation ecosystem can also foster innovation and creativity in the field of cybersecurity, leading to the development of new and effective solutions to meet evolving cyber threats.

- **Ethical and responsible data management**: Emphasising the importance of ethical and socially responsible access, use, sharing, and management of data, especially while using AI tools, to ensure the protection of personal information and promote trust in technology. Ethical and responsible data management helps to protect the personal information of individuals and maintain trust in technology. Ensuring that data is collected, used, shared, and managed in an ethical, legal and socially responsible manner helps to protect privacy and promote public confidence in the use of technology. By stressing the importance of ethical data management, it can also foster innovation and encourage the development of new technologies, including AI technologies, that are both useful and trustworthy.

This project was funded by the European Union's Internal Security Fund – Police Programme under Grant Agreement No 101038738.

THE DECLARATION PRINCIPLES

- **Technology as an enabler**: Recognising the role that technology can play in increasing the reporting of cybercrime and improving the response to these incidents. Technology is considered an enabler in addressing the issue of cybercrime because it has the potential to improve the efficiency and effectiveness of reporting incidents and responding to them. The use of technology can provide faster and more accurate ways to identify and track cybercrime, which can ultimately lead to a more rapid response and resolution of the issue. Additionally, acknowledging technology as an enabler can also help raise awareness about the importance of addressing cybercrime and promoting the development of new technologies and solutions to tackle the issue.

- **Interoperable digital platforms**: Promoting interoperable digital platforms based on open standards and technical specifications, Application Programming Interfaces (APIs), and shared data models to enhance the overall security of the online world. Interoperable digital platforms promote compatibility and integration between different systems, allowing for seamless exchange of information and collaboration between different stakeholders. This can help to enhance the overall security of the online world by reducing the risk of errors, and inefficiencies that can arise from incompatibility between systems. The use of open standards and APIs also promotes transparency and fairness in the development and implementation of these platforms, ensuring that they are accessible to a wide range of stakeholders and can be used to support a diverse range of applications and services.

- **Closing the digital divide**: Encouraging the uptake of these solutions to close the digital divide and reduce inequalities, ensuring that everyone has equal access to the benefits of technology and the Internet. Closing the digital divide helps to reduce inequalities and ensure that everyone has equal access to the benefits of technology and the Internet. This can help to create a more inclusive and equitable society, where everyone has the opportunity to participate in the digital world, exercise his/her digital rights and enjoy its benefits, such as improved access to information, communication, education, and economic opportunities. By addressing the digital divide, we can help to create a more level playing field for all individuals and communities, regardless of their socio-economic status, location, or other factors. This can have positive impacts on a range of areas, including social and economic development, innovation, and individual empowerment.

This project was funded by the European Union's Internal Security Fund – Police Programme under Grant Agreement No 101038738.

THE DECLARATION PRINCIPLES

THE SIGNATORIES WILL STRIVE TOWARDS FOLLOWING GOALS:

FINANCIAL

- Developing sustainable measures to contribute, on a voluntary basis, to increase the reporting of cybercrime in the EU.
- Adopting and implementing of common solutions on a large scale to enhance the reporting of cybercrime and improve the overall security of the online world.
- Optimising synergies between EU, national, regional, and local funds to maximise the impact of their investment.
- Strengthening investment in local transformation from EU funds and programs to help in an inclusive and sustainable approach to cybersecurity.
- Using common procurement practices to jointly construe specifications and aid in reducing the cost of investing in successful solutions and related technologies.

TECHNICAL

- Using a commonly agreed list of standards and technical specifications to achieve interoperability of data, systems, and platforms in reporting and tracking of cybercrime.
- Making key enablers of effective reporting and tracking of cybercrime, including data, infrastructure, and services, available to all participants.
- Utilising a common marketplace to share data, digital services, and solutions related to reporting and tracking of cybercrime among SMEs, industries, associations, LEAs, and CERTs.

LEGAL

- Assessing the legislative measures needed to provide a common EU framework for cross-sector and cross-border reporting and tracking of cybercrime, and take steps to help in implementing such measures.

This project was funded by the European Union's Internal Security Fund – Police Programme under Grant Agreement No 101038738.