Security of Personal Data Processing Event

October 8th 2018, **Fabio GUASCONI**
European DIGITAL SME Alliance

European DIGITAL SME Alliance
123 Rue du Commerce| 1000, Brussels, Belgium

www.digitalsme.eu | office@digitalsme.eu

Speaker introduction

Fabio GUASCONI

- Chairman DIGITAL SME WG27K working group
- UNINFO (Italian standardization body for ICT) board of directors
- President UNINFO CT 510 - ISO/IEC JTC1 SC27 mirror
- CLUSIT board of directors
- SBS expert
- CISA, CISM, PCI-QSA, ITIL, PRINCE2, ISFS, Lead Auditor 27001 & 9001
- Partner and co-founder @ **Bl4ckswan** S.r.l.

Giving a voice of European digital SMEs

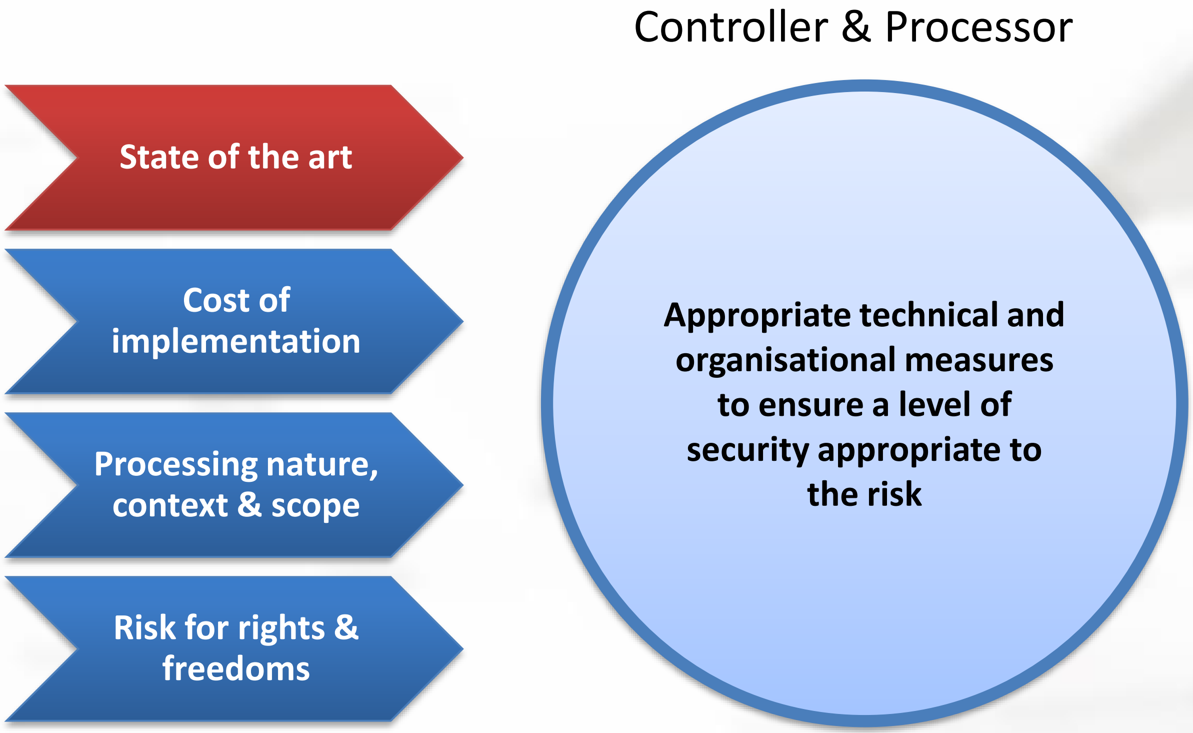
European DIGITAL SME Alliance

- The first European association in the ICT sector **exclusively focused on SMEs**
- Founded in 2007 from an initiative of **UEAPME**, the EU Association of SMEs
- Members are national associations of digital SMEs and ICT clusters from **19 countries**
- Representing over **20.000 enterprises**, across Europe
- Member of UEAPME, SBS, ECSO and AIOTI
- Now active on several **topics**: cybersecurity, ICT standardisation, digital taxation, digital skills, data economy, digitisation of industry...

Defining the state-of-the-art with regard to art. 32 GDPR

European
DIGITAL SME
Alliance

Article 32 scheme



Controller & Processor

State of the art

Cost of implementation

Processing nature, context & scope

Risk for rights & freedoms

Appropriate technical and organisational measures to ensure a level of security appropriate to the risk

What is the state-of-the-art

From the Oxford dictionary: "**The most recent stage in the development** [of a product]**, incorporating the newest ideas and the most up-to-date features**"

Therefore today a good approach could be to investigate security measures frameworks International information security and data protection standards and guides like:

- ISO/IEC 27002 and related ones (29151, 27018, upcoming 27552)
- NIST SP 800-53, BSI IT-Grundschutz, Cyber Essentials
- ENISA Guidelines
- SME Guide for the implementation of ISO/IEC 27001[1]

[1] https://www.digitalsme.eu/digital/uploads/SME-Guide-for-the-implementation-of-ISOIEC-27001-on-information-security-management-min-1-1-1.pdf

What is the state-of-the-art

Some common areas among the previously identified security measures frameworks are:

- Security organization
- Access control
- Asset management
- Data security
- Logging and monitoring
- Incident management
- System security
- Application security
- Physical security
- Network security
- Third-party security

What framework to choose?

No single choice among the previously mentioned ones is significantly better than the others for the purposes of article 32 as long as they are correctly implemented **within a risk management framework**.

Among factors that could anyways be considered for choosing one of them there are:

- **Regulatory or contractual requirements**
- **Stakeholders preferences** (e.g. controlling entities or business partners)
- **Available competences** (both internal and external)
- **Business opportunities** (e.g. participation to RFPs, competitive advantage)
- **Sectorial culture**

European
DIGITAL SME
Alliance

Conclusions

All this considered:

I. **The most relevant security measures frameworks are an adequate base for defining an appropriate set of technical and organizational measures.**

II. **An appropriate set of technical and organizational measures can only be deemed as such if it is proportional to the risk.**

III. **An effective risk management process must be in place to allow a balanced choice of an appropriate set of technical and organizational measures.**

European DIGITAL SME Alliance

THANKS FOR YOUR ATTENTION

fabio.guasconi@bl4ckswan.com