Quadro normativo ed obblighi di legge per uno studio professionale/impresa

La sicurezza e i rischi

- Tutte le organizzazioni raccolgono, elaborano **DATI** oggetto del Business

- I dati possono essere oggetto di
  - **PERDITA**
  - **FURTO**

- Da “il Gazzettino” del 14.11.2020

Il caso Tante le aziende venete vittime dei nuovi "rapitori"

Pirati informatici: 35 aziende ricattate

Spunti dalla normativa Europea

EUROPA		ITALIA			
TITOLO	**DATA**	**TITOLO**	**DATA**	**Note**	**Link**
EIDAS – Regolamento UE 910/2014 - Electronic IDentification Authentication and Signature	23.07.2014 efficace da 01.07.2016 obbligatorio da 29.09.2018	Da Codice Amministrazione Digitale D.Lgs. 82/2005 – Firme Digitali – ID Elettronica – Marche Temporali – PEC – SPID - CIE – Servizi Fiduciari.		Firme Digitali – ID Elettronica – Marche Temporali – PEC – SPID - CIE – Servizi Fiduciari.	https://www.eid.gov.it/?lang=it https://www.agid.gov.it/it/piattaforme/eidas
Direttiva NIS – EU 2118/2016 - (Network and Information Security) EU Member states have to supervise the cybersecurity of critical market operators in their country)	2016	D.P.C.M. 17.02.2017 (Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali.) - D.Lgs 18.05.2018 (Attuazione NIS) – D.P.C.M. 08.08.2019 Attivazione CSIRT (Computer Security Incident Response Team)	06.05.2020	*La direttiva individua sette settori strategici che sono strettamente legati alla dimensione della sicurezza, ossia energia, trasporti, banche, mercati finanziari, sanità, fornitura e distribuzione di acqua potabile e infrastrutture digitali, oltre a motori di ricerca, cloud e piattaforme online.*	https://www.enisa.europa.eu/ https://csirt.gov.it/
Direttiva 680/2016 – EU 689/2016	05.05.2016 efficace da 06.05.2018	D.Lgs. 51/2018	18.05.2018	*Trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali*	
RGDP – EU 679/2016	24.05.2016 efficace da 25.08.2018	**L. 196/2003 modificata da D.Lgs. 101/2018**	18.08.2018	Regolamento Europeo in materia di Protezione Dati Personali. Art 32 SICUREZZA DEL TRATTAMENTO	https://www.garanteprivacy.it/home

Impatto per uno studio

- Le norme si qui ricordate disciplinano:
  - COMUNICAZIONE
  - TRATTAMENTO
  - SICUREZZA

  nell'organizzazione del SISTEMA DIGITALE in GENERALE
- INTERESSANO le piccole realtà operative IMPONENDO:
  - la SICUREZZA del TRATTAMENTO dei DATI PERSONALI

Passi obbligatori per tutti

- Da GDPR e' prevista:
  - protezione dei dati fin dalla progettazione (art. 25);
  - data loss e leak prevention (DLP) sia per le funzioni sia per le modalità (artt. 25 e 32);
  - application security (art. 25);
  - sicurezza del trattamento dei dati (art. 32 commi 1 e 2).

Utilità derivante dalle NORMATIVE

- Sebbene non COGENTI le normative sulla Sicurezza per la Pubbliche Amministrazioni, almeno in alcuni punti, possono risultare UTILI per l'ORGANIZZAZIONE degli uffici
  - le MISURE MINIME DI SICUREZZA (https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict)
- Analogamente la conoscenza del sistema di SICUREZZA DIGITALE NAZIONALE può dare informazioni utili (https://csirt.gov.it/)

Misure Minime di Sicurezza

Indice delle azioni (AgID-Circolare 18 aprile 2017, n. 2/2017)

- ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI
- ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI
- ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER
- ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ
- ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE
- ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE
- ABSC 10 (CSC 10): COPIE DI SICUREZZA
- ABSC 13 (CSC 13): PROTEZIONE DEI DATI

- Previsti 3 livelli M-Minimo S-Standard A-Avanzato

Le PERDITE e la SICUREZZA

- Se i dati di lavoro sono perduti il danno è certo
- Unica soluzione è data dalla corretta FORMAZIONE del personale e dalla presenza di opportuni sistemi:
  - Tracciamento - Log
  - Salvataggio - BackUp
  - Sistemi di sicurezza (mail / antivirus / ..)

Uno Strumento “INSOLITO”

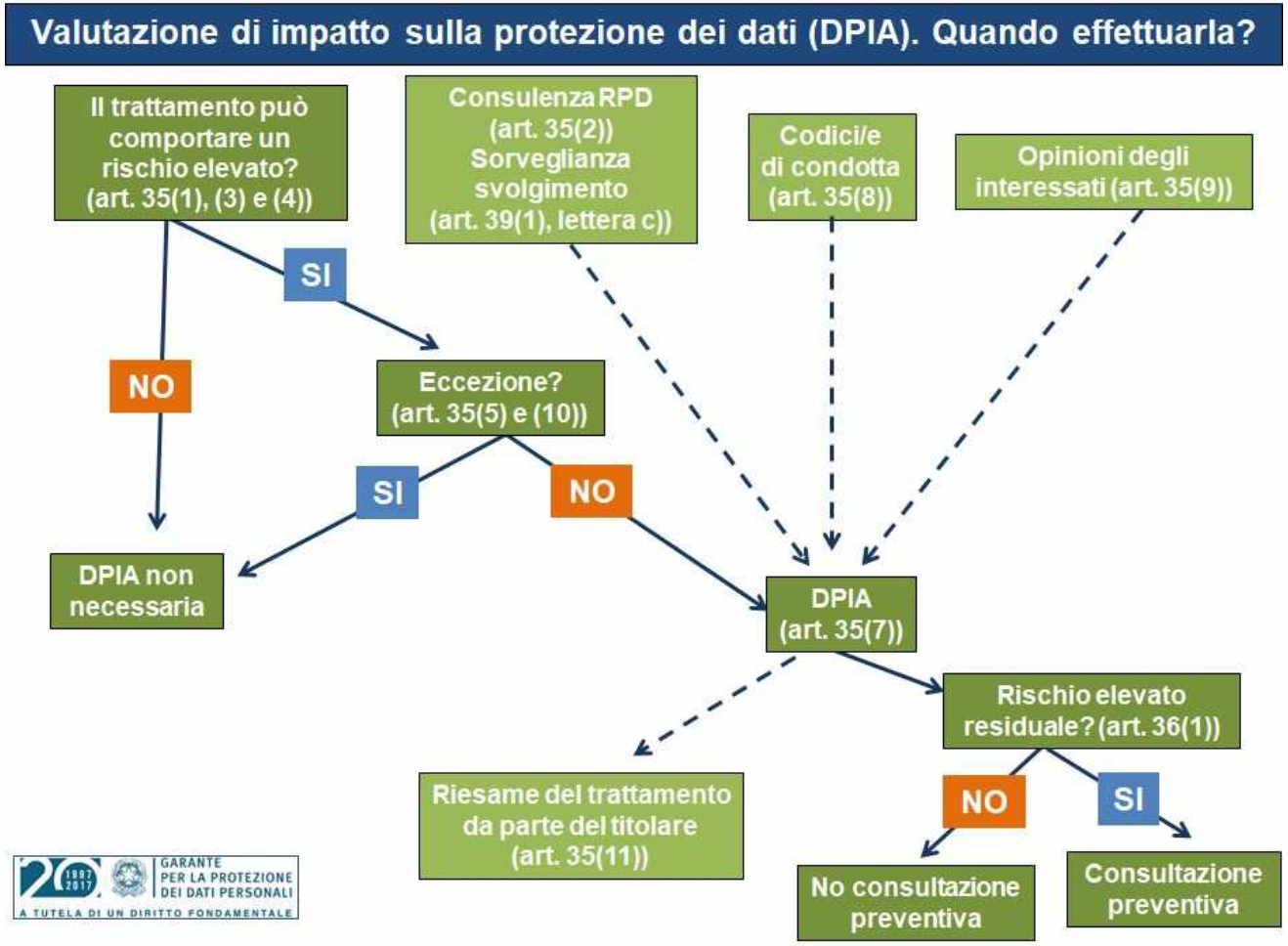
- La SICUREZZA digitale non può prescindere dall’ORGANIZZAZIONE del LAVORO

La normativa sulla PRIVACY impone l’analisi delle procedure organizzative e suggerisce l’uso del DPIA (Data Protection Impact Assessment) (Art. 35 GDPR – per specifiche tipologie di dati)

Il software - gratuito e liberamente scaricabile dal sito www.cnil.fr https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil offre un percorso guidato alla realizzazione della DPIA, secondo una sequenza conforme alle indicazioni fornite dal WP29 nelle Linee-guida sulla DPIA.

Schema DPIA

- Al solo scopo di dare una idea del processo di analisi si riporta:
-



Grazie per l'attenzione

Piero Bernardi
bernardipiero@libero.it