IL GDPR E LE MISURE MINIME DI SICUREZZA AGID

Franco Sivilli
fsivilli@unich.it

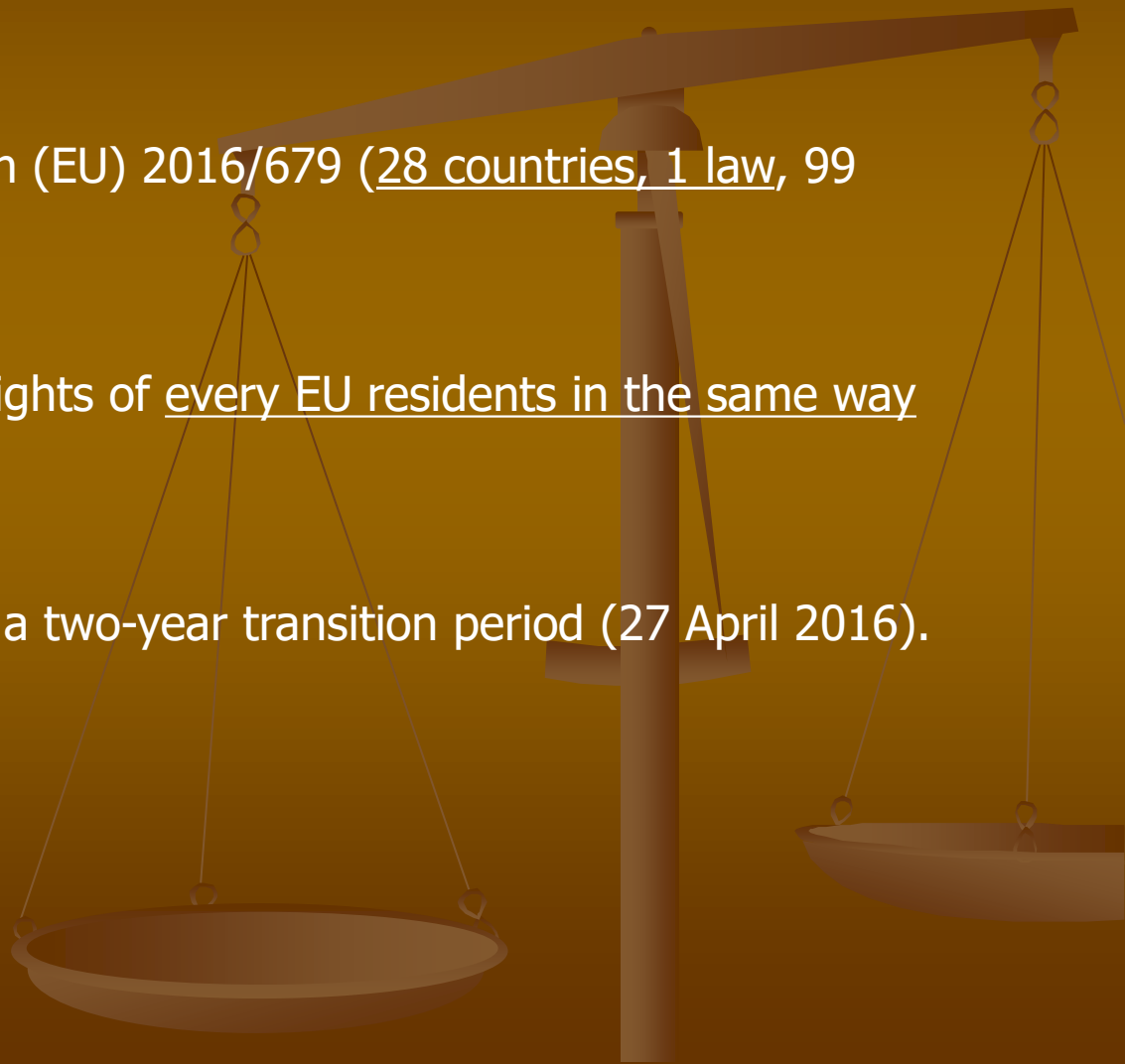
IL GDPR

GDPR FAQ

What?
General Data Protection Regulation (EU) 2016/679 (28 countries, 1 law, 99 Articles).

Why?
A regulation which regulates the rights of every EU residents in the same way with regard to their personal data.

When?
It applies from 25 May 2018 after a two-year transition period (27 April 2016).

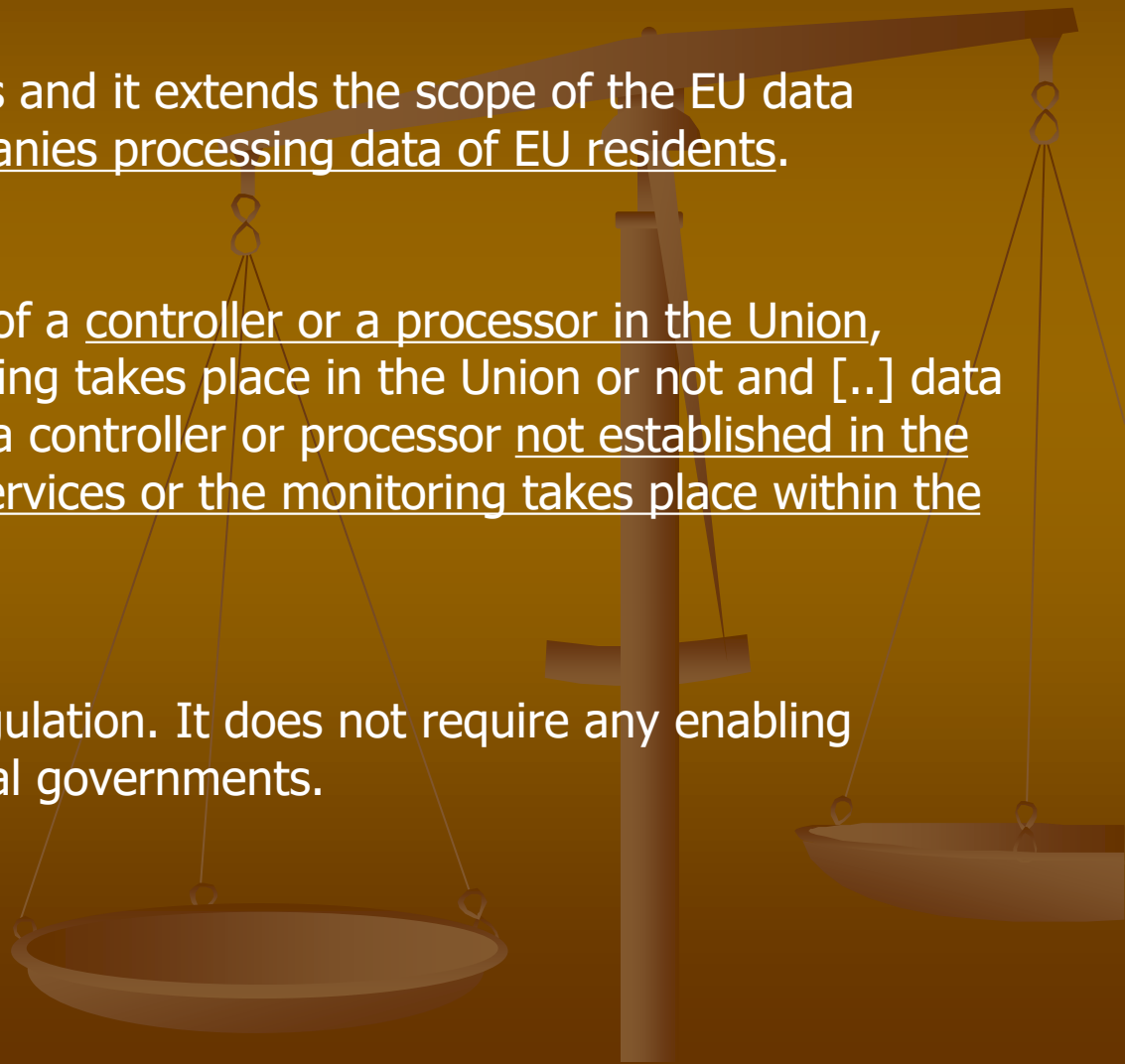


GDPR FAQ

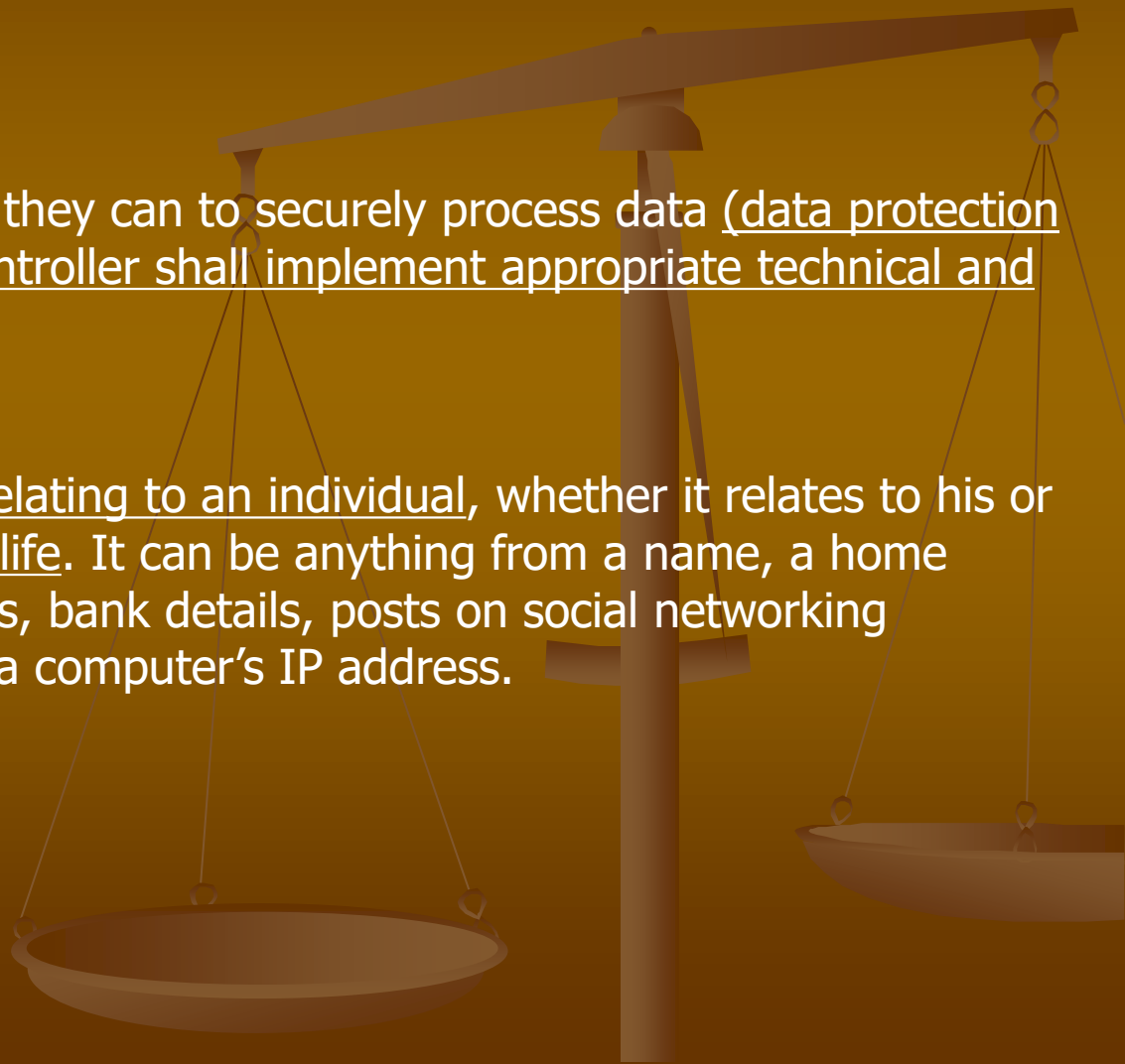
Where?
Wherever. EU based organizations and it extends the scope of the EU data protection law to all foreign companies processing data of EU residents.

Who?
[..] Activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not and [..] data subjects who are in the Union by a controller or processor not established in the Union and: offering of goods or services or the monitoring takes place within the Union.

Changes?
This is not a directive, this is a regulation. It does not require any enabling legislation to be passed by national governments.



GDPR FAQ



How?
Companies need to do everything they can to securely process data (data protection by design and by default). The controller shall implement appropriate technical and organisational measures.

Personal Data?
Personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address.

GDPR FAQ

Art. 4 – Definitions

'**controller**' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

'**processor**' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

'**processing**' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Sanctions

(Article 83 Par. 4) Up to 10,000,000 EUR or up to 2% of the annual worldwide turnover of the preceding financial year in case of an enterprise

(Article 83 Par. 5,6) Up to 20,000,000 EUR or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise

Rights of the data subject

Art. 12 - Informed Consent Criteria
The controller shall take appropriate measures to provide any information relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. [..] The controller shall provide information on action taken on a request within one month of receipt of the request.

Art. 15 - Right of Access
the right to obtain from the controller confirmation as to whether or not personal data and access to the personal data

Art. 16 - Right to rectification
the right to obtain from the controller without undue delay the rectification of inaccurate personal data

LAW

Rights of the data subject

Art. 17 - Right Erasure (Right To Be Forgotten)
the right to obtain from the controller the erasure of personal data

Art. 20 - Right to Data Portability
the right to receive the personal data

Art. 21 - Right to Object
the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data

Accountability and Data Protection

Art. 24 – Responsibility of the controller

the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

Art. 25 - Data Protection by Design and By Default

The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons

Data Protection Officer (DPO Art. 37)

Mandatory appointment:

- Core business activities involve regular and systematic monitoring of data subjects or processing of sensitive personal data on a large scale.
- Applies to both controllers and processors.
- EU Member States may introduce broader DPO requirements.
- DPO is formally tasked with ensuring that an organization is aware of, and complies with, its data protection responsibilities.
- DPO enjoys significant independence in performing tasks (no instructions, no dismissal or other disciplinary action).

Security

Art. 32 – Security of processing

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Breach Notification

Art. 33 - Notification of a personal data breach to the supervisory authority
In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority

Art. 34 - Communication of a personal data breach to the data subject
When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

State-of-the-art

Dictionary:
The latest and **most sophisticated or advanced stage of a technology**, art, or science.

Cambridge dictionary:
Very modern and using the **most recent ideas and methods**.
A state-of-the-art computer
The control panel uses all the **newest technology** and is considered state-of-the-art.

Dizionari Corriere:
Di altissimo livello, di punta, modernissimo, avanzato.

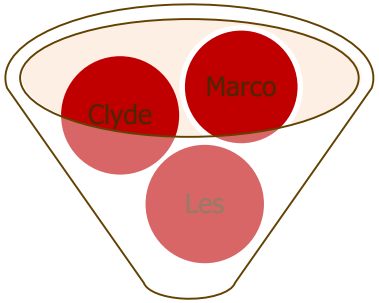
Wikipedia:
La locuzione stato dell'arte deriva dall'espressione anglosassone *state of the art*, ma ha un significato diverso rispetto all'originale. In italiano esisteva già in precedenza, nella contrattualistica privata, il concetto di regola dell'arte, o **regola d'arte**.

Other GDPR aspects

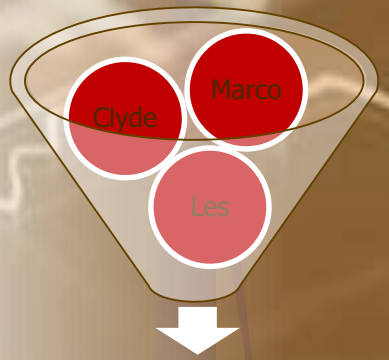
- **Compliance Documentations**
- **Data Anonymization**
- **Data Pseudonymisation**
- **Data Erasure**
- **Data Portability**
- **Data Access**

Pseudonymization versus Anonymization

"**Pseudonymization** is a method to substitute identifiable data with a reversible, consistent value. **Anonymization** is the destruction of the identifiable data."



Pseudonymized Data Record



Anonymized Data Record

Name	Token/Pseudonym	Anonymized
Clyde	qOerd	xxxxx
Marco	Loqfh	xxxxx
Les	Mcv	xxxxx

AGID – MISURE MINIME DI SICUREZZA

Misure Minime di Sicurezza ICT per la PA

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri
Area Sistemi, tecnologie e sicurezza informatica

MISURE MINIME DI SICUREZZA ICT

PER LE PUBBLICHE AMMINISTRAZIONI

(*Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015*)

Logica dei requisiti minimi

Il livello minimo è quello al quale ogni pubblica amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme. I livelli successivi rappresentano situazioni evolutive in grado di fornire livelli di protezione più completi, e dovrebbero essere adottati fin da subito dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visti come obiettivi di miglioramento da parte di tutte le altre organizzazioni.

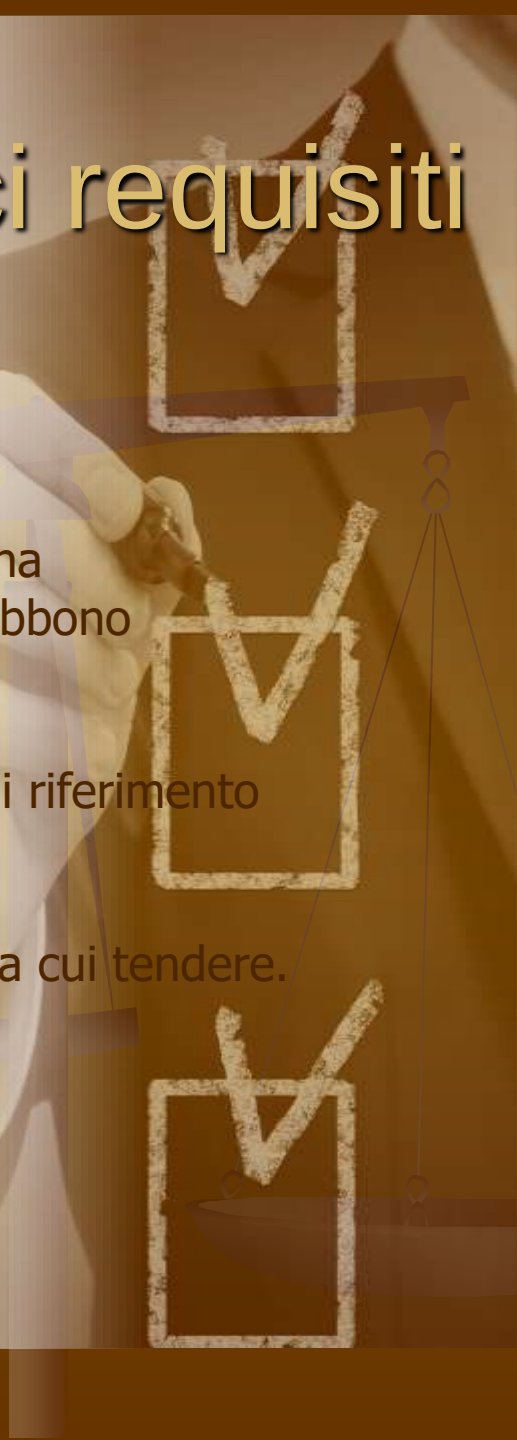
Otto temi con molteplici requisiti per ogni tema

Ogni singolo requisito è classificato:

La prima, «**Minimo**», specifica il livello sotto il quale nessuna amministrazione può scendere: i controlli in essa indicati debbono riguardarsi come obbligatori.

La seconda, «**Standard**», può essere assunta come base di riferimento nella maggior parte dei casi,

Mentre la terza, «**Alto**», può riguardarsi come un obiettivo a cui tendere.



Misure Minime di Sicurezza ICT per la PA – Punto 1

ABSC 1 (CSC 1) INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	ID.AM-1	X	X	X
		2	Implementare ABSC 1.1.1 attraverso uno strumento automatico	ID.AM-1		X	X
		3	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	ID.AM-1			X
		4	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	ID.AM-1			X
	2	1	Implementare il "logging" delle operazione del server DHCP.	ID.AM-1		X	X
		2	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	ID.AM-1		X	X
	3	1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1	X	X	X
		2	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1		X	X
	4	1	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	ID.AM-1	X	X	X
		2	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	ID.AM-1		X	X
		3	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	ID.AM-1			X

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
1	5	1	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	ID.AM-1			X
	6	1	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	ID.AM-1			X

Misure Minime di Sicurezza ICT per la PA – Punto 2

ABSC 2 (CSC 2) INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
2	1	1	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	ID.AM-2	X	X	X
	2	1	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	ID.AM-2		X	X
		2	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	ID.AM-2		X	X
		3	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	ID.AM-2			X
	3	1	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	ID.AM-2	X	X	X
		2	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	ID.AM-2		X	X
		3	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	ID.AM-2			X
	4	1	Utilizzare macchine virtuali e/o sistemi air-gapped1 per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	ID.AM-2			X

Misure Minime di Sicurezza ICT per la PA – Punto 3

ABSC 3 (CSC 3) PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE

Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vul- nerabilita` di servizi e configurazioni.

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
	1	1	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	PR.IP-1	X	X	X
		2	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	PR.IP-1		X	X
ABSC_ID #			**Descrizione**	**FNSC**	**Min.**	**Std.**	**Alto**
3	5	1	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	PR.DS-6		X	X
		2	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	PR.DS-6			X
		3	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.	PR.IP-3			X
		4	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	PR.IP-3			X
	6	1	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	PR.IP-3			X
	7	1	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	PR.IP-3			X

Misure Minime di Sicurezza ICT per la PA – Punto 4

ABSC 4 (CSC 4) VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilita`, correggere e minimizzare la finestra di opportunita` per gli attacchi informatici.

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
			Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su				
ABSC_ID #			**Descrizione**	**FNSC**	**Min.**	**Std.**	**Alto**
4	5	1	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	PR.MA-1	X	X	X
		2	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	PR.MA-1	X	X	X
	6	1	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	ID.RA-1 DE.CM-8		X	X
	7	1	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	PR.IP-12 RS.MI-3	X	X	X
		2	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	PR.IP-12 RS.MI-3		X	X
	8	1	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	ID.RA-4 ID.RA-5 PR-IP.12	X	X	X
		2	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	PR.IP-12	X	X	X
	9	1	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	PR.IP-12 RS.MI-3		X	X
	10	1	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	PR.DS-7		X	X

Misure Minime di Sicurezza ICT per la PA – Punto 5

ABSC 5 (CSC 5) USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
ABSC_ID #			**Descrizione**	**FNSC**	**Min.**	**Std.**	**Alto**
	6	1	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	PR.AC-1 PR.AT-2			X
			Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative				
ABSC_ID #			**Descrizione**	**FNSC**	**Min.**	**Std.**	**Alto**
5	10	1	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	ID.AM-6	X	X	X
		2	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	ID.AM-6	X	X	X
		3	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	ID.AM-6 PR.AT-2	X	X	X
		4	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	ID.AM-6 PR.AT-2		X	X
	11	1	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	PR.AC-1 PR.AT-2	X	X	X
		2	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	PR.AC-1 PR.AC-2	X	X	X
			giato i singoli comandi.				
	9	1	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	PR.AT-2 PR.PT-2 PR.PT-3 PR.PT-4		X	X

Misure Minime di Sicurezza ICT per la PA – Punto 6

ABSC 8 (CSC 8) DIFESE CONTRO I MALWARE

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
8	5	1	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	DE.CM-1 DE.CM-4		X	X
		2	Installare sistemi di analisi avanzata del software sospetto.	DE.CM-4			X
	6	1	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	DE.CM-1 DE.CM-4		X	X
	7	1	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	PR.PT-2	X	X	X
		2	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	PR.AT-1 DE.CM-4	X	X	X
		3	Disattivare l'apertura automatica dei messaggi di posta elettronica.	PR.AT-1 DE.CM-4	X	X	X
		4	Disattivare l'anteprima automatica dei contenuti dei file.	PR.AT-1 DE.CM-4	X	X	X
	8	1	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	PR.PT-2 DE.CM-4	X	X	X
	9	1	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	DE.CM-1 DE.CM-4	X	X	X
		2	Filtrare il contenuto del traffico web.	DE.CM-1 DE.CM-4	X	X	X
		3	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	DE.CM-1 DE.CM-4	X	X	X
	10	1	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	DE.CM-1 DE.CM-4		X	X
	11	1	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	ID.AM-6 DE.CM-4 RS.CO-5		X	X

Misure Minime di Sicurezza ICT per la PA – Punto 7

ABSC 10 (CSC 10) COPIE DI SICUREZZA

Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di neces- sità.

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
10	1	1	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	PR.IP-4	X	X	X
		2	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	PR.IP-4			X
		3	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	PR.IP-4			X
	2	1	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	PR.IP-4		X	X
	3	1	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud. .	PR.DS-6	X	X	X
	4	1	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	PR.AC-2 PR.IP-4 PR.IP-5 PR.IP-9	X	X	X

Misure Minime di Sicurezza ICT per la PA – ABSC 13

ABSC 13 (CSC 13) PROTEZIONE DEI DATI

Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
13	1	1	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	ID.AM-5	X	X	X
	2	1	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	ID.AM-5 PR.DS-5		X	X
	3	1	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	ID.AM-3 PR.AC-5 PR.DS-1 DE.AE-1			X
	4	1	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	ID.AM-3 DE.CM-1			X
	5	1	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	PR.PT-2			X
		2	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	ID.AM-1 PR.PT-2			X
	6	1	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	ID.AM-3 DE.CM-1			X
		2	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	ID.AM-3 DE.CM-1			X
	7	1	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	ID.AM-3 PR.DS-5 DE.CM-1			X
	8	1	Bloccare il traffico da e verso url presenti in una blacklist.	ID.-AM3 PR.DS-5 DE.CM-1	X	X	X
	9	1	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	PR.AC-4 PR.DS-5			X

SUMMARY AND RECOMMENDATIONS

GDPR (home page)
http://www.eugdpr.org/

GDPR (articoli)
https://gdpr-info.eu/

GDPR Guida del Garante della Privacy
http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali

Grazie per l'attenzione

Franco Sivilli
fsivilli@unich.it