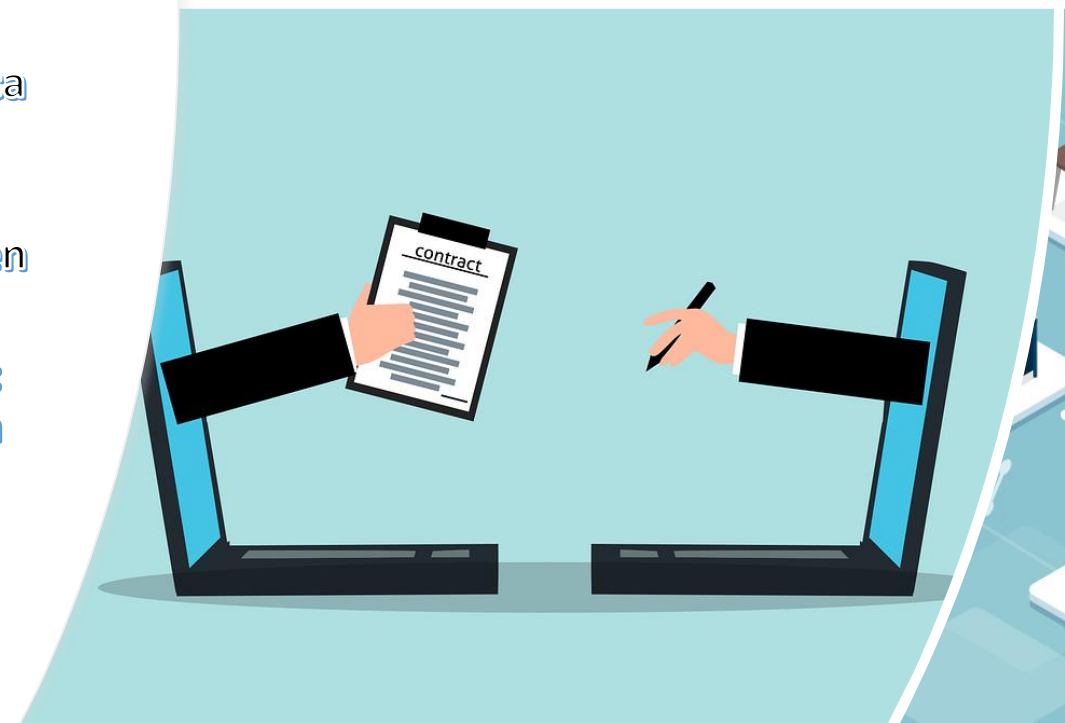
FORMAZIONE PRIVACY ai sensi dell'art. 29 GDPR

- Privacy: adempimenti, normativa e aggiornamenti
- La conservazione digitale a norma e le linee guida AgID
- Il codice di condotta sulla protezione dei dati nella pratica dello smart working
- La documentazione per l'obbligo di esibizione del Green Pass
- Il tema della cybersicurezza: etica, normativa e soluzioni da adottare



NOVEMBRE 2021

Riferimenti normativi e Faldone Privacy

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 - DECRETO LEGISLATIVO 10 agosto 2018, n. 101	Allegato A0 Conservazione digitale
Nomine a Responsabili Esterni del trattamento	Allegato A1
Registro delle attività di trattamento	Allegato A2
Mappatura delle sedi e delle interconnessioni	Allegato A3
Analisi dei rischi	Allegato A4
Valutazione di impatto (DPIA)	Allegato A5
Nomine di incarico di autorizzazione al trattamento(Art. 4.10 – Art. 28.b – Art. 29 GDPR)	Allegato A6
Nomina responsabile del sistema informatico, custode delle password, custode delle chiavi e altre nomine	Allegato A7
Codice di condotta per i soggetti autorizzati al trattamento dei dati personali (Art. 40 GDPR) e Altri Codici di condotta	Allegato A8
Altri codici di Condotta (Art. 40 GDPR)	Allegato A9
Provvedimento in materia di videosorveglianza - 8 aprile 2010 ed eventuale Documentazione relativa ai sistemi di videosorveglianza (ove prevista)	Allegato A10
Schede e dichiarazioni di adeguamento dei fornitori di prodotti software/hardware	Allegato A11
Misura di sicurezza degli edifici e dell'architettura di rete del sistema informatico	Allegato A12
Interventi formativi e documentazione	Allegato A13
Informative e consenso al trattamento	Allegato A14
Aggiornamenti/Scadenze/Verbali	Allegato A15
Documentazione relativa ai Trasferimenti di dati personali verso paesi terzi o Organizzazioni internazionali (CAPO V GDPR)	Allegato A16

TITOLARE

- ADOTTARE POLICY SULLA PRIVACY RISPETTANDO LA NORMATIVA GDPR (ANALISI DEI RISCHI VALUTAZIONE DI IMPATTO) – UTILIZZARE SOFTWARE CERTIFICATI E SISTEMI DI CYBERSICUREZZA EVOLUTI
- REDIGERE E TENERE AGGIORNATO (ANCHE IN FORMA DIGITALE) IL REGISTRO DELLE ATTIVITA' DI TRATTAMENTO/LA MAPPATURA DELLE SEDI E DEGLI ASSET
- AUTORIZZARE I DIPENDENTI AL TRATTAMENTO
- NOMINARE DIPENDENTI/ESPERTI AD INCARICHI SPECIALI
- NOMINARE I RESPONSABILI ESTERNI
- PROMUOVERE LA FORMAZIONE
- VERBALIZZARE I CASI DI VIOLAZIONE DEI DATI E PROVVEDERE A PRENDERE LE MISURE

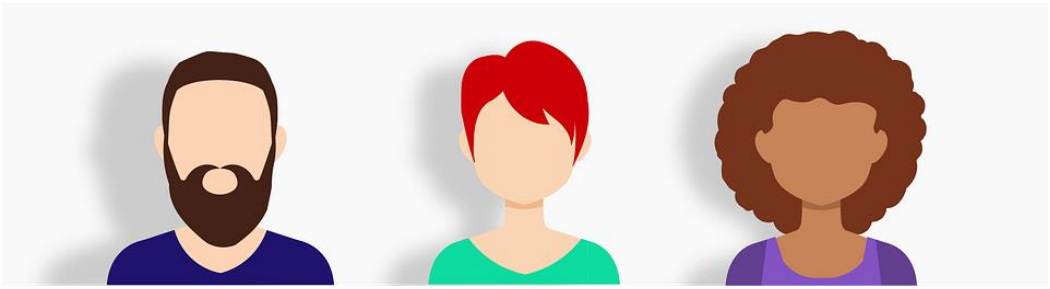
DIPENDENTE

ALLA CESSAZIONE DEL RAPPORTO DI LAVORO:

- REVOCA DELLE PASSWORD

- INFORMATIVA (CONSENSO)
- CODICE DI CONDOTTA AZIENDALE
- NOMINA DI AUTORIZZAZIONE AL TRATTAMENTO DEI DATI/REGISTRO DEI TRATTAMENTI DI COMPETENZA/MAPPATURA SEDE-ASSET
- NOMINE PARTICOLARI (RESPONSABILE DEL SISTEMA INFORMATICO, CUSTODE DELLE PASSWORD, CUSTODE DELLE CHIAVI)
- FORMAZIONE
- COMUNICARE AL TITOLARE I CASI DI VIOLAZIONE DEI DATI PERSONALI PER COMPILARE IL REGISTRO DATA BREACH E PRENDERE TEMPESTIVAMENTE I PROVVEDIMENTI

CLIENTI FORNITORI O ALTRI SOGGETTI INTERESSATI AL TRATTAMENTO



- INFORMATIVA (CONSENSO SE PREVEDE MARKETING O RACCOLTA DI DATI PARTICOLARI)
- RICHIESTA DELL'INFORMATIVA DEI CLIENTI/FORNITORI

ALLA CESSAZIONE DEL RAPPORTO/SERVIZIO, SE RICHIESTO:

RISPONDERE ALL'ESERCIZIO DEI DIRITTI CON:

- RETTIFICA/CANCELLAZIONE DEI DATI
- OBLIO
- TRASFERIBILITA' DEI DATI

Fatto salvo il legittimo interesse del Titolare

NOTA:

Registro Pubblico delle Opposizioni. La regolamentazione del marketing Telefonico e cartaceo D.P.R. n. 178/2010 e successive modificazioni

RESPONSABILE ESTERNO

INTERVENIRE SU EVENTUALI REVOCHE DI PASSWORD E ACCESSI AI SISTEMI AZIENDALI ALLA CESSAZIONE DEL RAPPORTO, SE LO SI RITIENE OPPORTUNO, RICHIEDERE L'ESERCIZIO DEI DIRITTI DI:

- RETTIFICA/CANCELLAZIONE DEI DATI
- OBLIO
- TRASFERIBILITA' DEI DATI

Fatto salvo il legittimo interesse del Responsabile Esterno

- NOMINA DI INCARICO A RESPONSABILE ESTERNO PER SERVIZI CHE RICHIEDONO IL TRATTAMENTO DEI DATI A CUI FA CAPO IL TITOLARE
- RICHIEDERE EVENTUALI CERTIFICAZIONI DI QUALITA' AL RESPONSABILE ESTERNO
- INTERVENIRE CON AZIONI DI MONITORAGGIO/CONTROLLO SUL SUO OPERATO

Risoluzione del Parlamento europeo del 25 marzo 2021 sulla relazione di valutazione della Commissione concernente l'attuazione del regolamento generale sulla protezione dei dati due anni dopo la sua applicazione.

Clicca qui https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_IT.html

1. **valuta positivamente il fatto che il GDPR sia diventato il riferimento mondiale in materia di protezione dei dati personali** e rappresenti un fattore di convergenza nell'elaborazione delle norme; si compiace del fatto che con l'adozione del GDPR l'UE abbia assunto un ruolo di primo piano nel dibattito internazionale sulla protezione dei dati e che diversi paesi terzi abbiano allineato al GDPR le proprie normative in materia di protezione dei dati

2. conclude che, due anni dopo la sua entrata in applicazione, il GDPR può essere globalmente considerato un successo e concorda con la Commissione sul fatto **che allo stato attuale non è necessario che sia sottoposto ad aggiornamento o riesame**;

3. riconosce che, fino alla prossima valutazione della Commissione, si dovrà continuare a **porre l'accento sul miglioramento dell'attuazione e sulle azioni volte a rafforzare l'applicazione del GDPR**;

4. prende atto della necessità di **un'applicazione rigorosa ed efficace del GDPR presso le piattaforme digitali**, le imprese integrate e altri servizi digitali di grandi dimensioni, in particolare nei settori della pubblicità online, del micro-targeting, della profilazione algoritmica, della classificazione, della diffusione e dell'amplificazione dei contenuti;

Risoluzione del Parlamento europeo del 25 marzo 2021 sulla relazione di valutazione della Commissione concernente l'attuazione del regolamento generale sulla protezione dei dati due anni dopo la sua applicazione.

Base giuridica del trattamento

5. esorta le autorità di controllo dei dati a precisare che i titolari del trattamento devono **fare affidamento su una sola base giuridica per ciascuna finalità** delle attività di trattamento, e a specificare in che modo ciascuna base giuridica sia invocata per le loro operazioni di trattamento
6. ricorda che, dall'inizio dell'applicazione del GDPR, **per "consenso" si intende qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato**; sottolinea che ciò si applica anche alla direttiva e-privacy
7. esprime preoccupazione per il fatto che il "legittimo interesse" è molto spesso citato in modo improprio come base giuridica del trattamento

Diritti degli interessati

8. sottolinea che è necessario **agevolare l'esercizio dei diritti individuali sanciti dal GDPR, tra cui la portabilità dei dati** e i diritti riguardanti il trattamento automatizzato in linea con il principio della minimizzazione dei dati e l'attuazione del diritto all'anonimato che previene efficacemente la divulgazione non autorizzata, il furto d'identità e altre forme di abuso dei dati personali;

9. evidenzia che il **rispetto del diritto** di essere informato impone alle imprese di fornire **informazioni in modo conciso, trasparente, intelligibile e facilmente accessibile**

Risoluzione del Parlamento europeo del 25 marzo 2021 sulla relazione di valutazione della Commissione concernente l'attuazione del regolamento generale sulla protezione dei dati due anni dopo la sua applicazione.

Piccole imprese e organizzazioni

10. osserva che alcune parti interessate segnalano che l'applicazione del GDPR è stata particolarmente complessa, specialmente per le piccole e medie imprese (PMI), ritiene che le campagne informative delle **autorità nazionali e della Commissione dovrebbero rendere disponibili una maggiore assistenza, informazione e formazione al fine di contribuire a migliorare le conoscenze, la qualità dell'attuazione e la consapevolezza dei requisiti e della finalità del GDPR**;

11. **sottolinea che non esistono deroghe per le PMI**, incoraggia l'EDPB (European Data Protection Board - Il Comitato europeo per la Protezione dei Dati) a sviluppare modelli di politica della privacy ad uso eventuale delle organizzazioni, in modo da aiutarle a dimostrare l'effettiva conformità al GDPR nella pratica

Attuazione

12. esprime preoccupazione dinanzi **all'attuazione disomogenea e talvolta inesistente del GDPR da parte delle autorità nazionali** di protezione dei dati a più di due anni dall'inizio dell'applicazione di tale regolamento, e si rammarica pertanto che, in termini di attuazione, la situazione non sia sostanzialmente migliorata;

13. prende atto del fatto che nei primi 18 mesi di applicazione del GDPR sono stati presentati circa **275 000 reclami e sono state imposte 785 sanzioni amministrative** per diverse violazioni, ma sottolinea che **finora è stato dato seguito solo in minima parte ai reclami presentati**

Risoluzione del Parlamento europeo del 25 marzo 2021 sulla relazione di valutazione della Commissione concernente l'attuazione del regolamento generale sulla protezione dei dati due anni dopo la sua applicazione.

14. esprime preoccupazione in relazione alla **durata delle indagini** condotte da alcune autorità di protezione dei dati e alle relative ripercussioni negative sull'efficacia dell'attuazione e la fiducia dei cittadini

15. è preoccupato in relazione al fatto che le autorità di controllo di 21 Stati membri dei 31 Stati che applicano il GDPR, vale a dire tutti gli Stati membri dell'Unione europea e dello Spazio economico europeo, e il Regno Unito, hanno dichiarato esplicitamente di **non disporre di risorse umane, tecniche e finanziarie, di locali e di infrastrutture sufficienti per adempiere efficacemente i loro compiti ed esercitare i loro poteri**

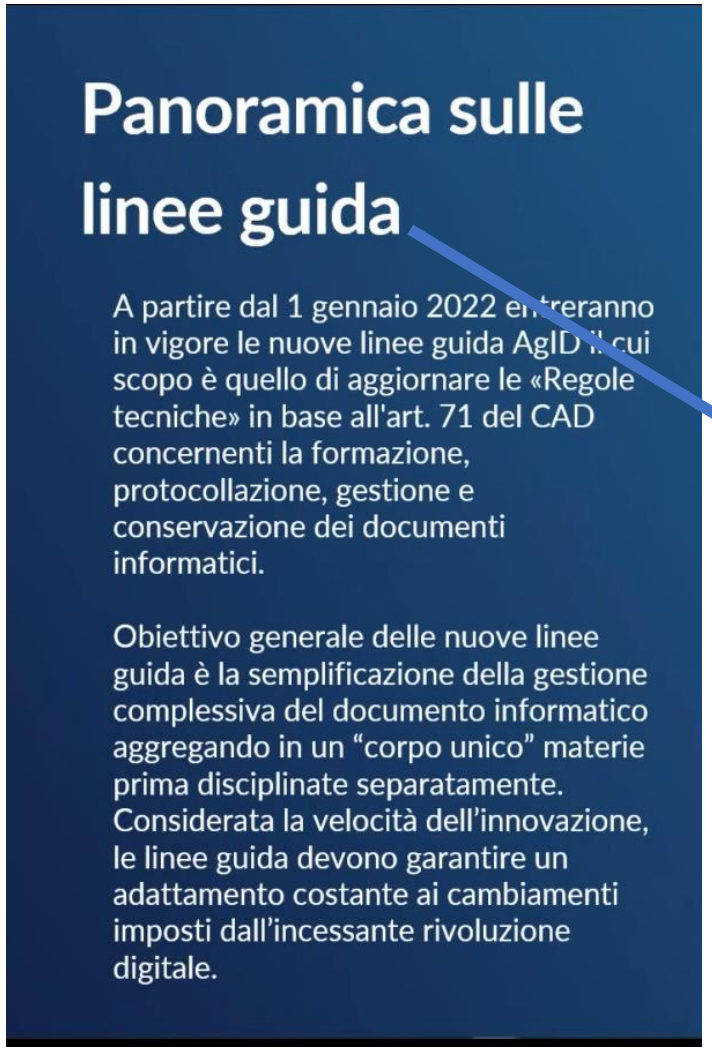
16. invita la Commissione a valutare la possibilità di obbligare le **grandi multinazionali tecnologiche** a pagare per la propria vigilanza introducendo una **tassa dell'UE sul digitale**;

17 - 18. si rammarica del fatto che la maggior parte degli Stati membri abbia deciso di non dare attuazione all'articolo 80, paragrafo 2, del GDPR; invita tutti gli Stati membri ad avvalersi dell'articolo 80, paragrafo 2, e **ad attuare il diritto di proporre reclami e di adire i tribunali senza essere incaricati da un interessato**;

ALTRI TEMI TRATTATI NELLA RISOLUZIONE

Cooperazione e coerenza
Frammentazione dell'attuazione del GDPR
Protezione dei dati fin dalla progettazione
Linee guida

La conservazione digitale a norma, termine e obbligo per l'adeguamento 1 gennaio 2022, con le linee guida emanate dall'Agenzia per l'Italia Digitale sulla formazione, gestione e conservazione dei documenti informatici.



Codice dell'amministrazione digitale

AGID Agenzia per l'Italia Digitale

Clicca qui https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_sul_documento_informatico.pdf

La conservazione digitale a norma

MANUALE DELLA CONSERVAZIONE

E' il documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

Clicca qui

https://www.agid.gov.it/sites/default/files/repository_files/documentazione/schema_manuale_conservazione_v2_1.doc

La conservazione digitale a norma

Creazione, versamento, archiviazione e distribuzione rappresentano i quattro processi fondamentali a cui è sottoposto ogni documento digitale durante il proprio percorso di vita. Il regolamento tecnico redatto dall'AgID, su deroga del CAD, stabilisce i requisiti tecnologici del sistema di conservazione necessari a garantire la validità legale del documento stesso.

Le normative italiana ed europea consentono la totale dematerializzazione dei documenti, processo che, tramite la conservazione digitale, intende sostituire integralmente i vecchi e ingombranti archivi cartacei con quelli digitali, più agili, economici e semplici da gestire.
Al fine di effettuare tale tipologia di conservazione documentale è necessario far ricorso a determinati strumenti (firma digitale e PEC, *marche temporali…*) e attenersi alle linee guida dell'AgID.

Pertanto, nelle linee guida sono stabiliti i requisiti tecnici affinché **un documento possa garantirsi autentico, integro, affidabile, leggibile e reperibile** e quindi valido sotto il profilo legale.

Ecco le quattro fasi del processo di conservazione sostitutiva o conservazione digitale a norma:
- Creazione → Produzione del documento digitale o trasformazione da analogico a digitale
- Versamento → Preparazione del Pacchetto di Versamento con le caratteristiche tecniche normate (firma digitale/marca temporale/compilazione dei metadati)
- Archiviazione → Acquisizione del PdV da parte del Conservatore, controlli ed esecuzione di procedure sul PdV per produrre il rapporto di versamneto con esito positivo, conservazione digitale dei PdV in Pacchetti di Archiviazione PdA
- Distribuzione → Messa a disposizione degli utenti abilitati del Pacchetto di distribuzione PdD per la consultazione dei dati

La conservazione digitale a norma

Fase 1 - La creazione del documento digitale
Possiamo definire il documento digitale in due tipi distinti:
- il **documento digitale nativo** è il documento che nasce già in formato digitale, non è la mera riproduzione di un documento cartaceo o grafico, **come avviene ad esempio per le fatture elettroniche o le PEC;**
- il **documento digitalizzato è invece il documento che è formato in via analogica e che è successivamente digitalizzato, come ad esempio un documento cartaceo che viene scansionato**.
La corretta creazione del documento digitale garantisce l'autenticità originaria dello stesso prima del suo trasferimento al sistema di Conservazione e alla sua successiva archiviazione

La conservazione digitale a norma

Fase 2 - Il versamento del documento digitale

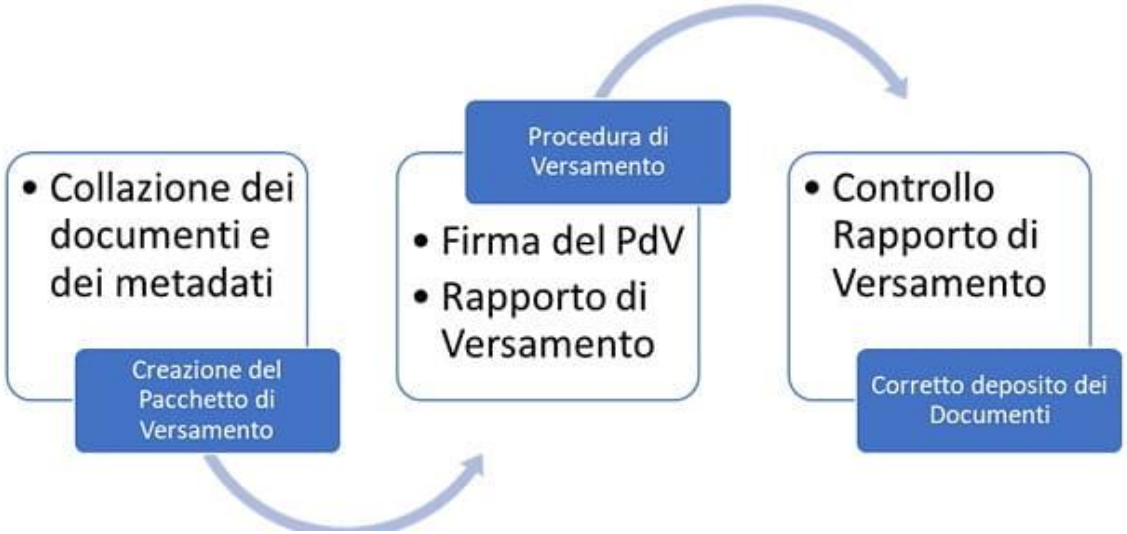
Il versamento rappresenta il momento di passaggio del documento digitale dal sistema che lo ha generato al sistema di conservazione.

Il processo di conservazione infatti è peculiare in quanto richiede, come prescritto dall'AgID, una serie di accortezze tecniche e tecnologiche che i conservatori in outsourcing posseggono essendo stati accreditati.

La fase di versamento consiste nell'inserire i documenti in una "cartelletta virtuale" nella quale sono collazionati, oltre ai documenti oggetto di conservazione, anche gli estremi di riferimento della documentazione (i metadati).

Questa "cartelletta", denominata **Pacchetto di Versamento (PdV),** viene firmata digitalmente e spedita, tramite procedimento telematico, al sistema di conservazione sostitutiva su cui viene infine archiviata, come stabilito nel **Manuale di conservazione**.

A questa fase segue l'esito del rapporto di versamento generato in automatico dal sistema di conservazione sostitutiva alla fine della procedura di versamento.



Metadati Obbligatori

- ✓ Modalità di formazione
- ✓ Tipologia Documentale
- ✓ Tipologia di flusso
- ✓ Tipo di registro
- ✓ Data di registrazione
- ✓ Numero documento
- ✓ Id registro (obbligatorio in relazione al tipo di registro)
- ✓ Oggetto
- ✓ Formato
- ✓ Mittente (obbligatorio in relazione alla tipologia di flusso e al tipo di registro)
- ✓ Autore (obbligatorio in relazione alla tipologia di flusso)
- ✓ Destinatario (obbligatorio in relazione al tipo di registro)
- ✓ Riservato
- ✓ Verifiche: firmato digitalmente, sigillato elettronicamente, marcatura temporale, conformità copie immagine su supporto informatico
- ✓ Versione del Documento
- ✓ Id Doc
- ✓ Allegati

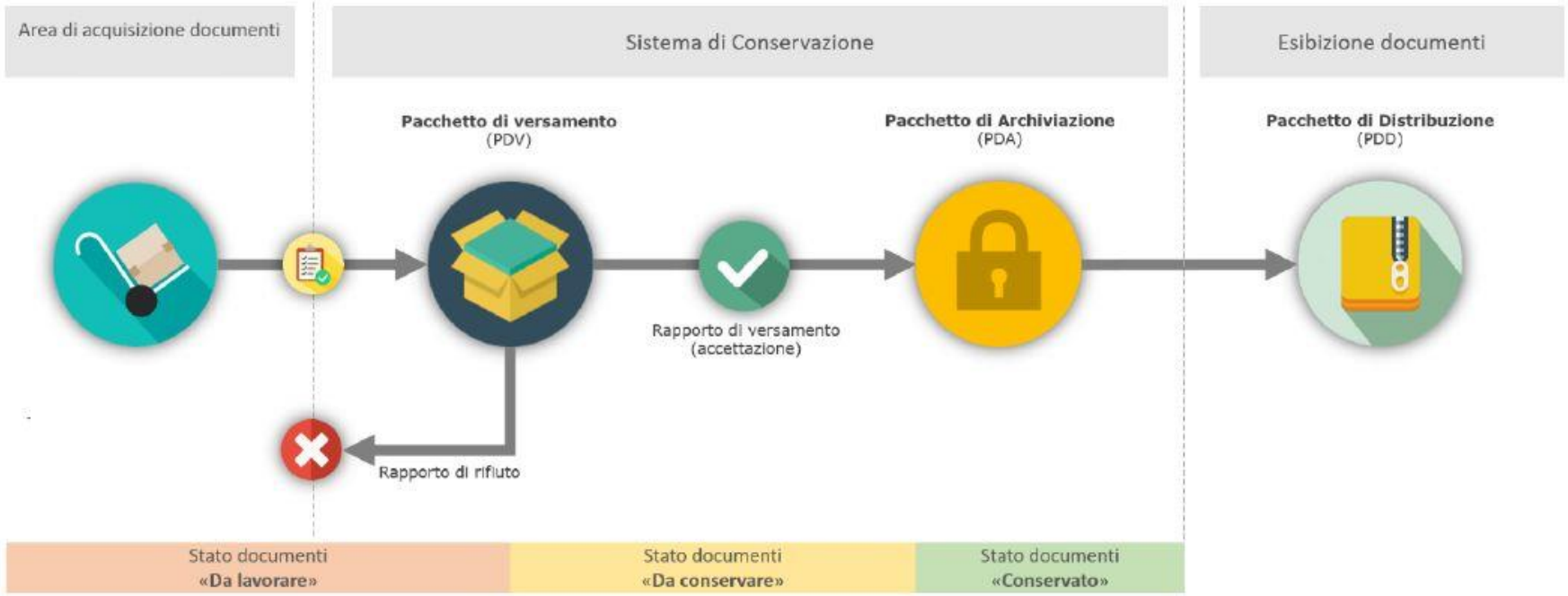
La conservazione digitale a norma

Fase 3 - L'archiviazione del documento digitale

Il PdV, una volta versato, è quindi archiviato nel sistema di conservazione sostitutiva ed è inserito all'interno di un più corposo "volume virtuale", chiamato Pacchetto di Archiviazione (PdA), nel quale sono raccolti svariati PdV della medesima tipologia documentale.

Ogni archivio ha diversi PdA, distinti per tipologia documentale e indicizzati (vale a dire catalogati e registrati) tramite le informazioni aggiuntive (metadati) inserite all'interno del volume e che ne denotano la composizione e la sua collocazione all'interno dell'archivio.

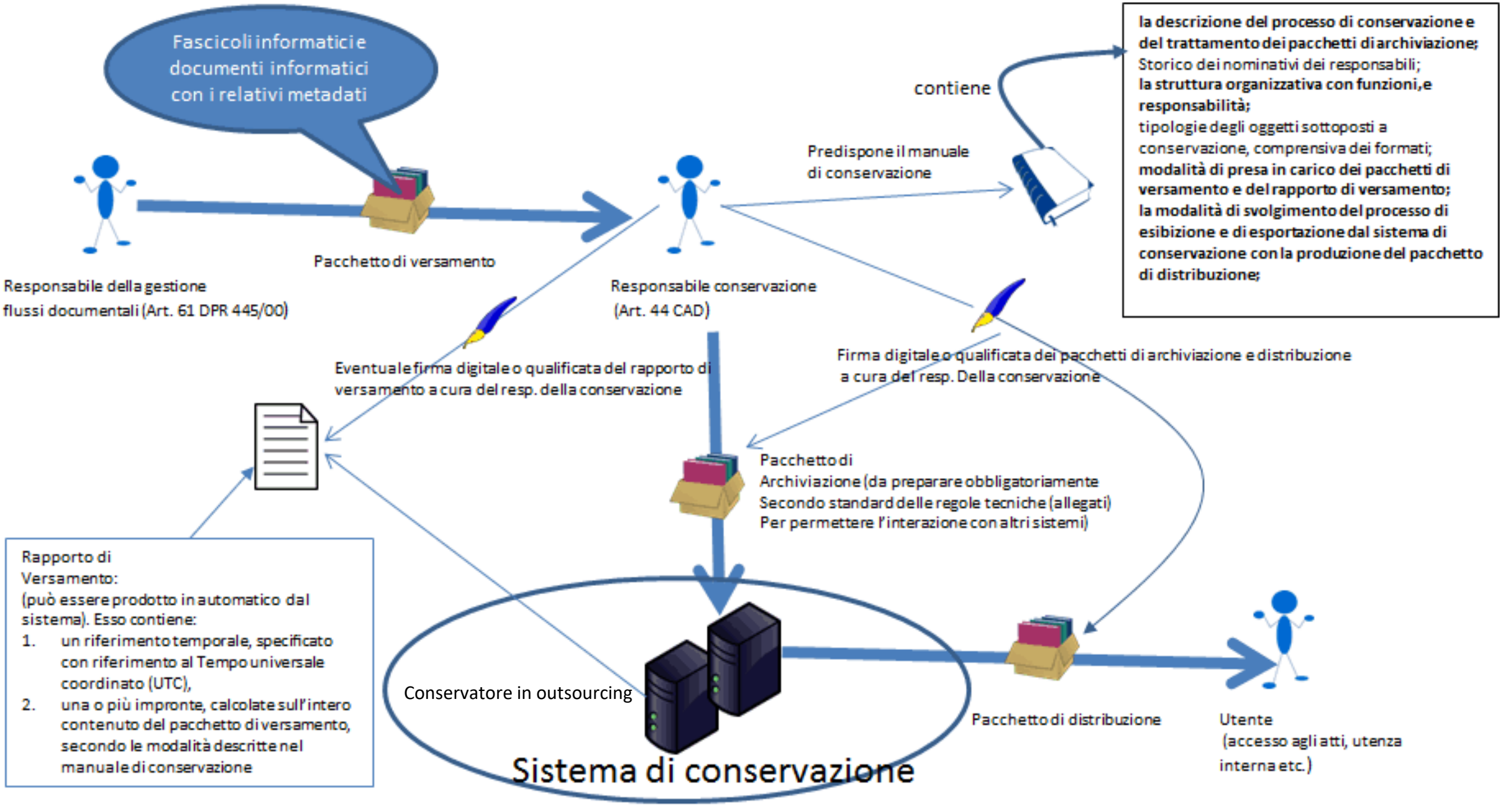
La funzione dei metadati ricorda, almeno in parte, quella delle etichette e delle linguette che si applicavano ai fascicoli negli archivi cartacei: identificare delle correlazioni, inserire delle note, segnalare delle notizie importanti ai fini della gestione dei documenti dell'archivio.



La conservazione digitale a norma

Fase 4 - La distribuzione del documento digitale
La fase finale del processo di gestione documentale digitale **consiste nella messa a disposizione, da parte del sistema di conservazione, dei documenti conservati ai soggetti che ne fanno richiesta**.
Questo passaggio del processo garantisce al soggetto che prende visione del documento tutte le caratteristiche proprie del documento digitale conservato a norma di
legge: autenticità, integrità, affidabilità, leggibilità e reperibilità.
Per ottenere questo risultato, anche in questo caso, infine, si ha la creazione di un pacchetto: il cosiddetto pacchetto di distribuzione (PdD). All'interno di esso sono presenti i documenti richiesti al sistema di conservazione sostitutiva, comprensivi dei rispettivi metadati.

La conservazione dei documenti informatici rilevanti ai fini fiscali, va eseguita entro una prestabilita scadenza, dato appunto che **va ultimata entro tre mesi dal termine ultimo di trasmissione delle dichiarazioni annuali**


Fascicoli informatici e documenti informatici con i relativi metadati
Pacchetto di versamento
Responsabile della gestione flussi documentali (Art. 61 DPR 445/00)
Responsabile conservazione (Art. 44 CAD)
Predispone il manuale di conservazione
contiene
la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
Storico dei nominativi dei responsabili;
la struttura organizzativa con funzioni, e responsabilità;
tipologie degli oggetti sottoposti a conservazione, comprensiva dei formati;
modalità di presa in carico dei pacchetti di versamento e del rapporto di versamento;
la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
Eventuale firma digitale o qualificata del rapporto di versamento a cura del resp. della conservazione
Firma digitale o qualificata dei pacchetti di archiviazione e distribuzione a cura del resp. Della conservazione
Pacchetto di Archiviazione (da preparare obbligatoriamente Secondo standard delle regole tecniche (allegati) Per permettere l'interazione con altri sistemi)
Rapporto di Versamento:
(può essere prodotto in automatico dal sistema). Esso contiene:
1. un riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC),
2. una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità descritte nel manuale di conservazione
Conservatore in outsourcing
Sistema di conservazione
Pacchetto di distribuzione
Utente (accesso agli atti, utenza interna etc.)

Per alcune tipologie di documenti aziendali la **Conservazione Digitale a norma di legge è obbligatoria:**

- **PEC**
- **Messaggi e ricevute di PEC**
- **Fattura elettronica**
- **Contratti firmati digitalmente**

Per altre tipologie, invece, la **Conservazione Digitale dei documenti a norma di legge è facoltativa**, ma consente di liberarsi dagli archivi cartacei e dagli obblighi e responsabilità della loro tenuta per **10 anni**, come previsto dal Codice Civile.

Tra questi troviamo:

- **Fatture**
- **DDT**
- **Ricevute fiscali**
- **Scontrini fiscali**
- **Bilancio d'esercizio (Stato Patrimoniale, Conto Economico, Nota integrativa, Relazione gestionale, Relazione sindaci e rev.)**
- **Dichiarazioni fiscali**
- **Modulistica pagamenti (ad esempio i modelli F23 e F24)**
- **Registri Contabili (ad esempio il Libro Giornale, i Registri IVA, i mastri, il libro inventari, etc.)**
- **Libro dei soci**
- **Libro delle obbligazioni**
- **Libro delle adunanze e delle deliberazioni**

Inoltre **è possibile archiviare qualsiasi altra tipologia di documento** secondo le proprie necessità, come ad esempio:

- **CUD**
- **Offerte**
- **Contratti**
- **Corrispondenza**
- **Documenti sanitari**
- **Documenti protocollati prodotti da Pubbliche Amministrazioni o da società soggette a obbligo di protocollazione informatica**
- **Mandati di pagamento e reversali**

La prima fase del processo è l'archiviazione documentale. Tale fase si sviluppa inizialmente con l'acquisizione ottica dei documenti cartacei e successivamente della loro memorizzazione su un supporto idoneo. L'archivio creato è quindi a disposizione per essere consultato al bisogno.

Conservazione sostitutiva e-fatture dell'Agenzia delle Entrate

Quando il numero di fatture elettroniche gestite in un anno è davvero esiguo, in alternativa al software, ci si può affidare al servizio gratuito di conservazione elettronica a norma, fornito dall'**Agenzia delle Entrate** : tutte le fatture emesse e ricevute transitate dal Sistema di Interscambio (SdI). Questo servizio è accessibile dal portale "Fatture e Corrispettivi" nella sezione "*Fatturazione Elettronica*" dove è presente il box "*Conservazione*". La funzione di conservazione è fruibile oltre che dal contribuente stesso, anche da terzi ufficialmente delegati secondo precise modalità previste dall'agenzia stessa.

Come aderire al servizio di conservazione delle fatture elettroniche?

Per poter usufruire di questo servizio occorre obbligatoriamente **aderire alla Convenzione** presente nel portale *Fatture e Corrispettivi*. Prima di accedere al servizio, infatti, il portale presenta la seguente schermata:

La convenzione ha durata di 3 anni e allo scadere deve essere rinnovata: il contribuente verrà avvisato prima della scadenza dal servizio stesso. Se il rinnovo viene fatto dopo la scadenza, le fatture emesse e ricevute nel periodo non coperto dalla convezione, dovranno essere portate in conservazione manualmente tramite l'upload presente nel sito stesso.

Dopo aver accettato i termini del servizio, tutte le fatture elettroniche relative del soggetto contribuente saranno **automaticamente inviate in conservazione**. Le fatture elettroniche vengono **conservate per 15 anni** dalla data di attivazione del servizio, anche in caso di mancato rinnovo, recesso o risoluzione, qualora non ne sia stata richiesta la restituzione completa (export).

Anche se ci si dota di un software di fatturazione elettronica completo di conservazione, è consigliabile **attivare sempre il servizio di conservazione offerto dall'Agenzia**, perché non comporta alcuna spesa e perché il Sistema d'Interscambio sarà sempre e comunque considerato la fonte ufficiale in caso di controlli.

LA CONSERVAZIONE DIGITALE IN OUTSOURCING

PRIMA PASSI DA SEGUIRE

CONSULTARE IL CONSULENTE DEL LAVORO E IL COMMERCIALISTA

CONSULTARE IL PROVIDER PEC

IL FORNITORE DEL SERVIZIO DI FATTURAZIONE ELETTRONICA

aruba.it BUSINESS

https://www.pec.it/acquista-conservazione-sostitutiva.aspx

InfoCert

https://www.infocert.it/conservazione/info/#responsabile

Namirial

https://www.namirial.com/it/trust-services/conserva-pec/

ARXivar ACTIVATE your business

https://www.arxivar.it/it/conservazione-sostitutiva/

Conservazione digitale dei documenti in house oppure in outsourcing

La conservazione digitale, che come rilevato deve essere eseguita seguendo pedissequamente le disposizioni contenute nel DMEF 17 giugno 2014 e nelle linee guida Agid del 9 settembre 2020, potrà essere svolta internamente all'organizzazione (cioè all'azienda o allo studio professionale), previa adozione di appositi software e avendo maturato le opportune competenze, oppure affidando il servizio all'esterno a operatori specializzati. In questo secondo caso, sarà necessario orientarsi verso conservatori in possesso di elevati livelli in termini di qualità, sicurezza e organizzazione accreditati Agid con certificazioni opportune.

Clicca qui

Codice di condotta per il trattamento dei dati personali al quale ci si deve attenere durante lo Smart Working.

In tale comunicazione dovranno essere definite le tecnologie utilizzate (sono da privilegiare **le tecnologie di Accesso Remoto/VPN/Cloud**) e i principali comportamenti da tenere nella condizione del lavoro agile.

Un valido suggerimento può essere quello dell'AGID che fornisce le seguenti **11 raccomandazioni per lo Smart Working sicuro**:

1. - Segui prioritariamente le policy, i codici di condotta e le raccomandazioni dell'Azienda
2. - Utilizza i sistemi operativi per i quali attualmente è garantito il supporto
3. - Effettua costantemente gli aggiornamenti di sicurezza del tuo sistema operativo
4. - Assicurati che i software di protezione del tuo sistema operativo (Firewall, Antivirus, ecc) siano abilitati e costantemente aggiornati
5. - Assicurati che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alle password policy emanate dalla tua Amministrazione
6. - Non installare software proveniente da fonti/repository non ufficiali
7. - Blocca l'accesso al sistema e/o configura la modalità di blocco automatico quando ti allontani dalla postazione di lavoro
8. - Non cliccare su link o allegati contenuti in email sospette
9. - Utilizza l'accesso a connessioni Wi-Fi adeguatamente protette
10. - Collegati a dispositivi mobili (pen-drive, hdd-esterno, etc) di cui conosci la provenienza (nuovi, già utilizzati, forniti dalla tua Amministrazione)
11. - Effettua sempre il log-out dai servizi/portali utilizzati dopo che hai concluso la tua sessione lavorativa.

Le indicazioni appena elencate sono da ritenersi relative sia nel caso di utilizzo di dispositivi personali (situazione prevista dal noto paradigma BYOD) quanto nel caso di dispositivi configurati e forniti dall'Azienda.

IL DATORE DI LAVORO DEVE FORNIRE AL LAVORATORE I SUPPORTI TECNOLOGICI PER ATTUARE LE MISURE

Le regole per l'eventuale uso di dispositivi personali per l'attività lavorativa (BYOD).

Lo smartphone e il portatile sono tecnologie ormai indispensabili nella vita quotidiana, da cui i possessori non si separano neanche durante le ore di lavoro. Interpretando questa tendenza, le imprese e le scuole hanno cercato di approfittarne e il risultato è il BYOD, l'integrazione dei dispositivi personali sul posto di lavoro o a scuola.
Negli ultimi anni se n'è parlato tanto, spesso sottolineando i grandi vantaggi per le imprese, ma il BYOD ha anche i suoi difetti, soprattutto dal punto di vista della sicurezza informatica e della protezione dei dati. Per questo motivo, sono nate tendenze anche opposte al BYOD.
L'acronimo BYOD sta per Bring Your Own Device, che in inglese significa "porta il tuo dispositivo".
Ad esempio, con una politica di BYOD, un'azienda può permettere ai dipendenti di svolgere il lavoro sui propri computer e smartphone, in ufficio e al di fuori di esso.
Le policy di BYOD sono state sviluppate con il chiaro obiettivo di aumentare la produttività dei dipendenti e migliorarne (teoricamente) le condizioni di lavoro, partendo dall'idea che un lavoratore si sente più a suo agio utilizzando il proprio computer o i dispositivi che conosce meglio e usa tutti i giorni. Inoltre, l'applicazione del BYOD flessibilizza l'orario lavorativo e si adatta anche bene al lavoro agile.
Nel caso delle aziende, l'obiettivo è quello di ridurre i costi di proprietà dell'hardware e di gestione delle infrastrutture IT, aumentando contemporaneamente la produttività dei lavoratori.

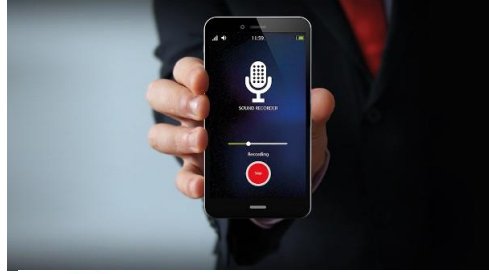
Il BYOD non ha solo vantaggi e presenta alcuni inconvenienti sia a livello di gestione di IT sia a livello di sicurezza dei dati. Per questo motivo, l'introduzione del BYOD in un'azienda dovrebbe sempre essere accompagnata dalla creazione una politica di BYOD, anche conosciuta come policy BYOD o linee guida BYOD (**Per questo, il Garante Europeo della protezione dei dati (EDPS) ha pubblicato delle linee guida per il BYOD).**

In sintesi si dovrebbe:

- **Definire quali dispositivi possono essere utilizzati e come.**
- **Definire i sistemi e le procedure di sicurezza per il BYOD.**
- **Descrivere i rischi di sicurezza relativi ai dati personali.**
- **Definire le responsabilità giuridiche di azienda e dipendenti relative all'utilizzo dei dispositivi.**
- **Stabilire la gestione finanziaria della proprietà e dei dispositivi.**
- **Creare sui dispositivi personali container o spazi delimitati per l'utilizzo aziendale, a cui vengono applicate tecnologie di sicurezza particolari come il blocco di servizi di terze parti, cifratura**
- **Accesso a desktop virtuali e ambienti di lavoro basati sul web che consentono l'accesso remoto al PC aziendale dai dispositivi personali, mantenendo al sicuro i dati.**

Alternativa al BYOD
il corporate-owned, personally enabled (in italiano "di proprietà aziendale, abilitato per l'uso personale"), conosciuto come COPE.
Il metodo COPE ha i seguenti vantaggi rispetto al BYOD:
L'azienda sceglie i dispositivi, riducendo i problemi di compatibilità e di gestione.
L'azienda possiede i dispositivi, per cui può disporne come meglio crede per proteggere i dati e l'accesso alle reti aziendali.
In conclusione, non è chiaro quale sarà il futuro del BYOD, ma è sicuramente destinato a rimanere, almeno in una certa misura. La penetrazione dei dispositivi digitali nella vita di tutti i giorni sta cambiando il concetto stesso di rapporto lavorativo e i modi in cui viene svolto il lavoro. Resta da vedere quali metodi daranno i migliori risultati sia per le aziende che per i lavoratori.

E’ lecito registrare una telefonata? Ecco cosa prevede il Codice Privacy



Registrare una conversazione all’insaputa dei presenti

È lecito registrare una conversazione che si intrattiene tra più persone ed all’insaputa di tutti o solo di alcuni. Chi parla accetta anche il rischio di essere registrato, dice la Cassazione. È però necessario che:

- alla conversazione partecipi colui che sta registrando, non ci può limitare a lasciare un sistema di registrazione e non essere presente;
- la registrazione non avvenga nei luoghi di privata dimora del «registrato», è illegale andare a casa di un amico o nel suo ufficio riservato e attivare la registrazione; bisognerebbe trovarsi in un luogo pubblico per attivare la registrazione
- é invece possibile registrare in casa propria quello che dicono invece gli ospiti.

Registrare una telefonata all’insaputa dell’altro

Così come è legale la registrazione di una conversazione tra presenti e all’insaputa di questi, la registrazione di una telefonata con un’altra persona ignara di essere “intercettata” non viola l’altrui privacy e, quindi, non costituisce reato.

Questo perché, secondo la Cassazione, la registrazione non fa che fissare, su una memoria elettronica, ciò che è già “nostro” e fa parte del nostro patrimonio sensoriale, essendo stato captato dal nostro udito e immagazzinato nella nostra memoria

Tale è stato anche l’orientamento espresso dalle Sezioni Unite della Cassazione nella famosa sentenza “apripista” del 2003 secondo cui la registrazione del colloquio, in quanto rappresentativa di un fatto, integra la prova documentale.

Posso far sentire ad altri o pubblicare la conversazione telefonica?

Se è legale registrare una telefonata, non lo è invece la pubblicazione del suo contenuto. Non si può quindi far ascoltare l’audio a una platea di uditori (ad esempio nel corso di una riunione di condominio), non si può pubblicare il file su internet o su un social network (a meno che si distorca il suono in modo da non far risalire all’autore della dichiarazione e vengano oscurati eventuali altri nomi citati nella conversazione). La legge vieta infatti solo la diffusione della conversazione salvo ci sia il consenso di tutti coloro che vi hanno partecipato (e non solo di uno).

Resta chiaramente lecito far sentire il contenuto della registrazione telefonica a un giudice, a un carabiniere, a un poliziotto e a qualsiasi altra autorità preposta alla tutela dei diritti del cittadino.

Ad esempio, è possibile fa ascoltare il file nel corso di un procedimento disciplinare dinanzi al proprio datore di lavoro; in una causa di separazione o divorzio per dimostrare, ad esempio, l’altrui confessione di tradimento; o in un giudizio per il recupero di un credito, per provare l’ammissione del debitore.

Sembrerà strano ma è proprio il Codice della Privacy a consentire la registrazione di una telefonata eseguita all’insaputa dell’altro conversante. Ciò infatti è necessario “per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento”.

Si può registrare una videoconferenza?

Le stesse regole previste per il telefono o lo smartphone valgono anche per le video conferenze. È lecito quindi registrare una chiamata via Skype o con qualsiasi altra applicazione per i video messaggi, fosse anche WhatsApp, Messenger, Zoom o altri.

DOCUMENTI necessari agli adempimenti derivanti dagli obblighi di esibizione del GREEN PASS previsti dal 15/10/2021

1) INFORMATIVA BACHECA GREEN PASS
2) COMUNICATO BACHECA GREEN PASS
3) Tali documenti andranno esposti in bacheca all'ingresso del luogo di lavoro.
3) NOMINA CONTROLLORE GREEN PASS che andrà compilato e fatto sottoscrivere ai controllori da Voi nominati.

Tutti i documenti di cui sopra, dovranno essere inseriti in copia in calce al faldone privacy in una cartella con titolo ADEMPIMENTI GREEN PASS

4) COMUNICAZIONE ASSENZA INGIUSTIFICATA da consegnare al lavoratore che si presenti in azienda sprovvisto di green pass valido (o senza green pass) a seguito dei controlli;
5) COMUNICAZIONE AL PREFETTO in caso di accertamento di violazione relative alla normativa Green Pass da parte degli incaricati

IMPORTANTE:
I documenti 4) e 5) andranno da Voi condivisi con il Vostro consulente del lavoro, che Vi invitiamo a contattare, tenendo presente che per le imprese con meno di quindici dipendenti, dopo il quinto giorno di assenza ingiustificata di cui al comma 6, art. 3 D.L. 127/2021, il datore di lavoro può sospendere il lavoratore per la durata corrispondente a quella del contratto di lavoro stipulato per la sostituzione, comunque per un periodo non superiore a dieci giorni, rinnovabili per una sola volta, e non oltre il termine del 31 dicembre 2021.

Il trattamento dati nell'attività di verifica del GREEN PASS/TEMPERATURA CORPOREA

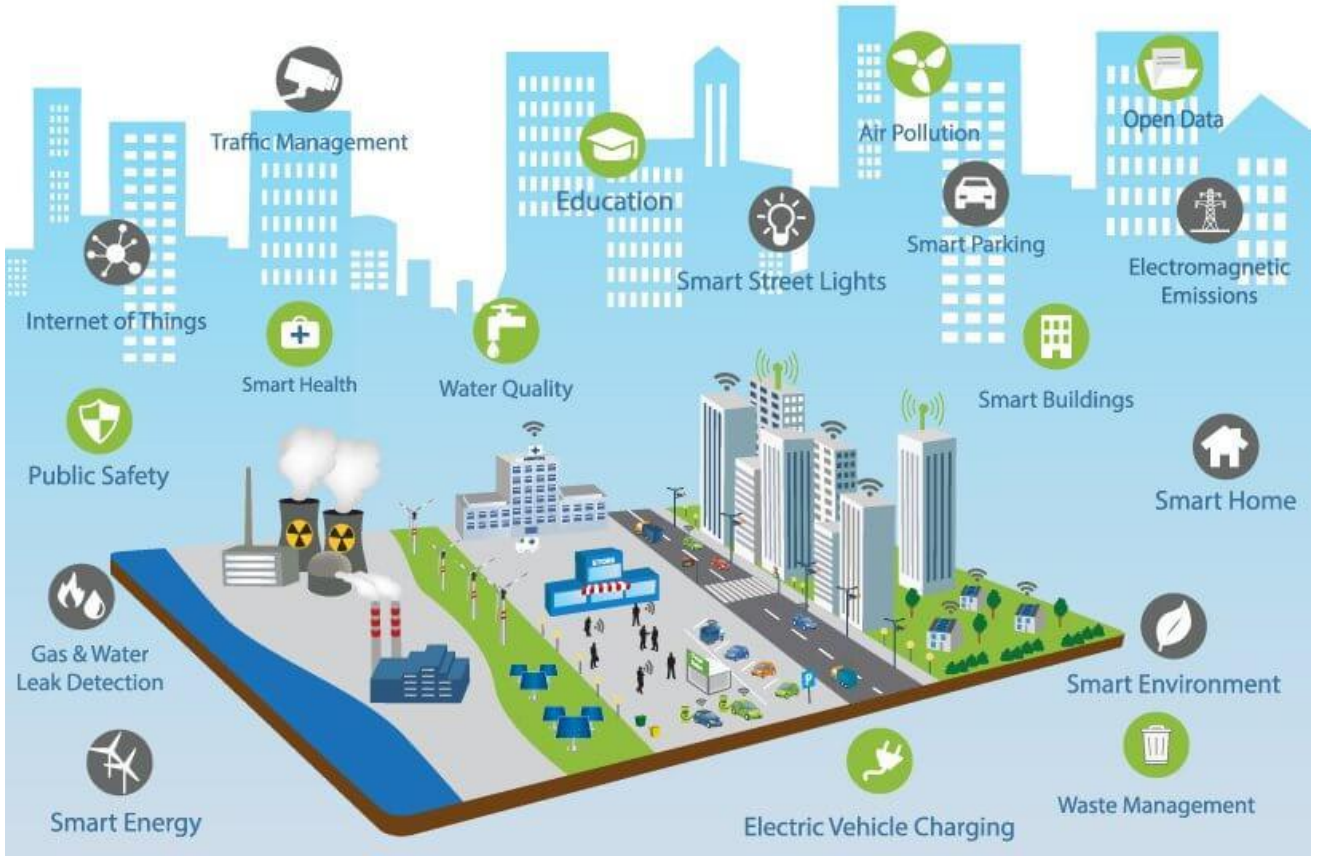
Nel provvedimento, il Garante coglie l'occasione di ribadire i limiti del trattamento dei dati personali degli interessati nell'ambito dell'attività di controllo del Green Pass.

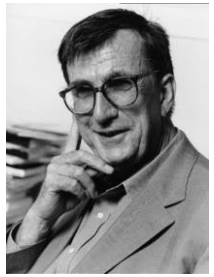
In particolare, il Garante afferma: "L'attività di verifica non dovrà comportare la raccolta di dati dell'interessato in qualunque forma, ad eccezione di quelli strettamente necessari, in ambito lavorativo, all'applicazione delle misure derivanti dal mancato possesso della certificazione. Il sistema utilizzato per la verifica del green pass non dovrà conservare il QR code delle certificazioni verdi sottoposte a verifica, né estrarre, consultare registrare o comunque trattare per altre finalità le informazioni rilevate".

Va quindi ribadito come ***non sia possibile per i datori di lavoro raccogliere "elenchi" di soggetti controllati o tenere "registri" da far compilare ai delegati al controllo****.*

L'attività di reporting del controllo effettuato, anche se a campione, non può comportare il trattamento di dati dei soggetti sottoposti a controllo e quindi è evidente che al delegato non potrà essere chiesto altro se non un'attestazione circa il fatto che lo stesso ha provveduto ad effettuare i controlli come da disposizioni ricevute e, nel caso di controlli a campione, quanti sono i soggetti da lui controllati (la rigidità della posizione del Garante si scontra però con la necessità di garantire la rotazione dei controlli, che imporrebbe quantomeno una comunicazione fra i delegati).

Pertanto riteniamo per ora di evitare la raccolta di dati in registri, la firma invece del registro degli accessi al luogo di lavoro/locali aziendali o la timbratura del cartellino di lavoro già determina che il controllo del GREEN PASS e l'eventuale controllo della temperatura abbiano avuto esito positivo altrimenti si procederà all'allontanamento del soggetto prendendo e notificando gli opportuni provvedimenti





Bruno Latour (Beaune, 22 giugno 1947) è sociologo, antropologo e filosofo francese.

http://www.bruno-latour.fr/sites/default/files/downloads/P-95-REGLES-ITAL.pdf

Le sue concezioni sui *non-umani* lo portano ad elaborare un programma di ecologia politica. Egli si augura che una nuova Costituzione prenda in considerazione non solo gli uomini ma anche i *non-umani*. Per questo, propone la creazione di un ***parlamento delle cose*** in cui le cose siano rappresentate da scienziati o personaggi riconosciuti per le loro competenze in un ambito particolare, allo stesso modo in cui i deputati tradizionali oggi rappresentano i cittadini.

Il tema della cybersicurezza per preservare i dati dal cybercrime e garantirne la conservazione e l'integrità; l'istituzione dell'Agenzia per la cybersicurezza nazionale (legge del 4 agosto 2021).

Clicca qui

https://threatmap.checkpoint.com/
https://www.webforma.it/news/top10-attacchi-informatici-primo-semestre-2021

Commissariato di P.S. online
Sportello per la sicurezza degli utenti del web

Che cosa prevede la nuova normativa italiana in tema di Cyber Security
È stata pubblicata in Gazzetta Ufficiale la **legge 4 agosto 2021, n.109 recante "Disposizioni urgenti in materia di cybersicurezza**, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale" che converte il decreto legge 14 giugno 2021, n. 82.

Il Governo, attraverso l'approvazione della legge, intende promuovere la cultura della sicurezza cibernetica e aumentare la consapevolezza sul tema all'interno del settore pubblico e privato, **accendendo i riflettori sui rischi e sulle minacce cyber**.

Negli ultimi anni, infatti, l'accresciuta esposizione alle minacce cibernetiche ha evidenziato la necessità di sviluppare, in tempi brevi, idonei e sempre più stringenti meccanismi di tutela e Cyber Security: nessun settore è immune da possibili cyber attacchi: **solo nel 2020, infatti, sono stati registrati 1.871 gli attacchi gravi di dominio pubblico, ovvero con un impatto sistemico in ogni aspetto della società, della politica, dell'economia e della geopolitica**.

Il pool di esperti che ha lavorato alla stesura del rapporto pone l'accento sull'incremento degli attacchi cyber a livello globale, che nel 2020 è pari a un +12% rispetto al 2019, e sull'aumento degli attacchi gravi con un +66% rispetto al 2017.

Tra i settori maggiormente colpiti ci sono il "Multiple Targets" (20% del totale degli attacchi), che comprende attacchi realizzati verso molteplici obiettivi spesso indifferenziati, il settore Governativo, militare, forze dell'ordine e intelligence (14% del totale degli attacchi), la sanità, (12% del totale degli attacchi), la ricerca e istruzione (11% del totale degli attacchi) e i servizi online (10% del totale degli attacchi). Inoltre, sono cresciuti gli attacchi verso Banking & Finance (8%), produttori di tecnologie hardware e software (5%) e infrastrutture critiche (4%).

In una società sempre più digitale, dove cresce il fenomeno della Gig Economy ed è impossibile fare a meno della tecnologia, quello della Cyber Security è uno dei temi più rilevanti dell'agenda nazionale ed internazionale.

La Cyber Security quindi è l'insieme dei mezzi, delle tecnologie e delle procedure utili a proteggere i sistemi informatici in termini di disponibilità, riservatezza e integrità dei dati e degli asset informatici. La cyber sicurezza costituisce uno degli interventi previsti dal Piano nazionale di ripresa e resilienza (PNRR) trasmesso dal Governo alla Commissione europea il 30 aprile 2021. Inoltre, è uno dei 7 investimenti della Digitalizzazione della pubblica amministrazione.

L'investimento, che mira alla creazione ed al rafforzamento delle infrastrutture legate alla protezione cibernetica del Paese, interessa quattro diverse aree:

1. **Rafforzamento dei presidi di front-line per la gestione degli alert e degli eventi a rischio verso la PA e le imprese di interesse nazionale;**
2. **Consolidamento delle capacità tecniche di valutazione e audit della sicurezza dell'hardware e del software;**
3. **Potenziamento del personale delle forze di polizia dedicate alla prevenzione e investigazione del crimine informatico;**
4. **Implementazione degli asset e delle unità incaricate della protezione della sicurezza nazionale e della risposta alle minacce cyber.**

I principali compiti dell'Agenzia sono:

- Promuovere la realizzazione di azioni comuni dirette ad assicurare la sicurezza e la resilienza cibernetiche per lo sviluppo della digitalizzazione del Paese, del sistema produttivo e delle pubbliche amministrazioni;
- Predisporre la strategia nazionale di cybersicurezza;
- Svolgere ogni necessaria attività di supporto al funzionamento del Nucleo per la cybersicurezza;
- Sviluppare capacità nazionali di prevenzione, monitoraggio, rilevamento e mitigazione, per far fronte agli incidenti di sicurezza informatica e agli attacchi informatici, anche attraverso il Computer Security Incident Response Team (CSIRT) italiano e l'avvio operativo del Centro di valutazione e certificazione nazionale;
- Curare e promuove la definizione ed il mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza, tenendo anche conto degli orientamenti e degli sviluppi in ambito internazionale;
- Contribuire all'innalzamento della sicurezza dei sistemi di Information and communications technology (ICT) dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica, delle pubbliche amministrazioni, degli operatori di servizi essenziali (OSE) e dei fornitori di servizi digitali (FSD);
- Supportare lo sviluppo di competenze industriali, tecnologiche e scientifiche, promuovendo progetti per l'innovazione e lo sviluppo e mirando a stimolare nel contempo la crescita di una solida forza di lavoro nazionale nel campo della cybersecurity in un'ottica di autonomia strategica nazionale nel settore.

1. **Creare un inventario**
2. **Individuare i sistemi critici.**
3. **Nominare un responsabile del sistema informatico.**
4. **Conoscere i regolamenti (attenersi al Codice di Condotta aziendale sulla privacy)**
5. **Formare il personale.**
6. **Fare attenzione al lavoro da remoto.**
7. **Installare antivirus.**
8. **Aggiornare software.**
9. **Fare più backup in «panieri diversi».**
10. **Stabilire una policy per le password.**
11. **Limitare i servizi web offerti da terzi.**
12. **Non condividere dati delicati all'esterno.**
13. **Controllare l'uso dei supporti rimovibili.**
14. **Proteggere con Firewall.**
15. **Non aprire link nelle email.**
16. **Policy BYOD e smart working.**
17. **Non cliccare sui pop up.**
18. **Proteggere il sito web.**
19. **Fare acquisti solo su siti sicuri.**
20. **Schermare la cam.**
21. **Controllare i post sui social media.**