Informazioni sul documento

Evidenza pubblica del documento: (pubblicato nella sottosezione web dipartimentale dedicata alla "Privacy e sicurezza")

Aggiornamento: giugno 2026

Sommario:

1. Finalità del documento

Categorizzare le informazioni dipartimentali in base al loro livello di sensibilità e criticità affinché i soggetti deputati al trattamento (sia in forma elettronica che fisica) possano utilizzarle nel modo più efficiente. Tale processo permette di applicare, laddove necessario, adeguate misure di protezione, nel pieno rispetto degli obblighi di conformità normativa. La finalità principale della politica di classificazione dei dati è quella di proteggere le informazioni sensibili, garantendone la conformità normativa ed ottimizzando la gestione delle risorse.

La presente politica è concepita come politica di classificazione delle informazioni di livello dipartimentale che disciplina la classificazione delle informazioni oltre il perimetro delle sole attività svolte in regime di delega per conto dell'Agenzia per le Erogazioni in Agricoltura (AGEA). La politica è sviluppata in coerenza con i requisiti di sicurezza previsti dalla Direttiva (UE) 2022/2555 (NIS2) e dalla relativa normativa nazionale di recepimento (D.Lgs. 4 settembre 2024, n. 138), nonché con le misure di sicurezza definite dall'Agenzia per la Cybersicurezza Nazionale (ACN).

2. Ambito di applicazione

Si applica a qualsiasi forma di dati ed informazioni, inclusi documenti cartacei e dati digitali memorizzati su qualsiasi tipo di supporto, trattati da soggetti interni ed esterni aventi titolo (dipendenti, collaboratori e/o persone o società autorizzate). La classificazione riguarda l'intero patrimonio informativo trattato, indipendentemente dal fatto che l'attività sia svolta in regime di delega per conto di AGEA o nell'ambito delle ordinarie funzioni istituzionali. Sebbene le informazioni abbiano un valore per l'amministrazione, non tutte hanno lo stesso valore o richiedono lo stesso livello di protezione. Individuare il valore delle risorse informative è fondamentale per comprendere il livello di sicurezza più appropriato, identificato il quale, è possibile implementare il controllo più idoneo per prevenire la perdita, il danneggiamento, il furto, la compromissione o interruzione delle attività. L'errata classificazione delle informazionipuò comportare l'implementazione di controlli inadeguati o non corretti a tutela delle stesse.

3. Classificazione delle tipologie di dati

I dati trattati dal Dipartimento dell'agricoltura si distinguono in:

1. **dati personali**
2. **dati non personali**

3.1 Dati personali

Per **dato personale** si intende qualsiasi informazione riconducibile, in modo univoco, a una persona identificata o identificabile. Anche le diverse informazioni che, raccolte insieme, possono portare all'identificazione di una determinata persona costituiscono dati personali (es: un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online, uno o più elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale).

I dati personali sottoposti ad anonimizzazione, cifratura o pseudonimizzazione, ma che possono essere utilizzati per reidentificare una persona, rimangono dati personali.

Esempio di dati personali:

- nome e cognome;
- indirizzo di residenza;
- indirizzo e-mail personale (es: nome.cognome@azienda.com);
- numero della carta d'identità;
- dati sulla posizione (ad es. la funzione di posizionamento su un telefono cellulare);
- indirizzo IP.

3.1.1 Categorie particolari di dati personali

Costituiscono **categorie particolari di dati personali** quelli che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Anche i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sono da considerarsi particolari e possono essere trattati soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

3.2 Dati non personali

I dati non personalisono informazioni che non si riferiscono a una persona fisica identificata o identificabile. Poiché non sono legati all'identità di alcun individuo, non sono soggetti alle restrizioni previste dal Regolamento Generale sulla Protezione dei Dati (GDPR)
Esempi di dati non considerati personali:

- numero di iscrizione al registro delle imprese di una società;
- indirizzo e-mail impersonale come info@azienda.com;
- dati resi anonimi in modo irreversibile (informazioni originariamente personali a cui vengono applicate tecniche di de-identificazione tali da impedire, in modo permanente e con qualsiasi mezzo, di risalire all'identità della persona fisica);
- territoriali, geografici e ambientali;
- mappe catastali prive dei riferimenti ai proprietari (particelle, confini, destinazione d'uso del suolo).
- meteorologici;
- statistici e demografici aggregati;
- dati amministrativi, gestionali e finanziari (bilanci)

Partendo dalle due categorie citate ai § 3.1 e 3.2 e tenuto conto delle peculiarità procedimentali afferenti il Dipartimento dell'agricoltura, sono state definite nove tipologie di dati ognuna con un livello di protezione adeguato al rischio ad essa associato. Le tipologie di dati elencate di seguito sono in ordine di rilevanza crescente sotto il profilo dell'impatto in caso di perdita di riservatezza, disponibilità e integrità dei dati. Il livello di protezione associato a ciascuna tipologia di dato può assumere uno dei seguenti quattro valori:

1. basso
2. medio
3. alto
4. molto alto

I livelli di protezione, descritti in un paragrafo successivo, sono definiti da un insieme di strumenti, procedure e sistemi di controllo adeguati a quel livello.

Tipo di dato	Descrizione	Livello di protezione	Esempio
Dati non personali (rischio basso)	sono dati generici solitamente destinati alla divulgazione pubblica attraverso applicativi web.	basso	• bandi • avvisi • informazioni sull'ente • dati aggregati • mappe • dati ambientali • dati meteorologici • dati statistici
Dati personali (tipo 1)	rientrano in questa categoria i dati personali che a seguito degli obblighi di pubblicità e trasparenza costituiscono oggetto di pubblicazione sul portale dipartimentale nel rispetto dei principi di "pertinenza e non eccedenza"(*minimizzazione*)	basso	• nome e cognome • dati reddituali e patrimoniali dei titolari di incarico • beneficiari di sovvenzioni e contributi
Dati personali (tipo 2)	Rientrano in questa categoria i dati personali per i quali non è prevista la pubblicazione	medio	• indirizzo residenza • recapito telefonico • dati bancari e finanziari • dati camerali • codici identificativi (c.f. e C.I.E.) • credenziali di accesso (password, PIN e codici di autenticazione usa e getta OTP)
Dati non personali (riservati/strategici)	Documentazione amministrativa, finanziaria o strategica dell'ente non destinata alla pubblicazione, la cui divulgazione anticipata o non autorizzata può causare danno reputazionale, economico o alterare procedure in corso.	alto	• documentazione pre-gara d'appalto (prima della pubblicazione) • audit interni di sicurezza • planimetrie dettagliate degli edifici dell'ente • report su vulnerabilità di sistema non ancora sanate.

Tipo di dato	Descrizione	Livello di protezione	Esempio
Dati particolari (*ad esclusione di quelli riferibili a tipologie successive*)	Sono dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare l'orientamento sessuale.	alto	• associazioni datoriali, sindacali o ordini professionali
Dati non personali (*infrastrutturali e di cybersicurezza*)	Informazioni tecniche e logiche la cui compromissione (furto, alterazione o distruzione) può mettere gravemente a rischio l'infrastruttura IT dell'ente, consentire accessi non autorizzati o interrompere l'erogazione di servizi critici.	molto alto	• mappature e topologie di rete • configurazioni di firewall e router • credenziali di amministrazione di sistema (sysadmin) • chiavi crittografiche • log di sicurezza • codici sorgente di applicativi critici proprietari
Dati biometrici	I dati personali ottenuti da un trattamento tecnico specifico e relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali i dati dell'immagine facciale o impronte digitali	molto alto	• immagini del volto • impronte digitali • timbro vocale • qualsiasi elemento fisico idoneo ad essere letto e interpretato da programmi di riconoscimento automatizzato
Dati sulla salute	I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute	molto alto	• patologie pregresse o in corso • referti medici • temperatura corporea

Tipo di dato	Descrizione	Livello di protezione	Esempio
Dati giudiziari	I dati che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale o la qualità di imputato o indagato. L'art.10 del GDPR ricomprende, in tale nozione, i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza. In particolare, rientrano in questa categoria i dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.	molto alto	• provvedimenti penali di condanna definitivi • libertà condizionale, • il divieto od obbligo di soggiorno, le misure alternative alla detenzione

4. Livelli di protezione dei dati ed informazioni contenute in documenti digitali

Per proteggere i dati con le adeguate misure di sicurezza, sono stati definiti dei livelli di protezione in termini di strumenti informatici, procedure e sistemi di controllo. Un capitolo a parte è dedicato, successivamente, alle misure di sicurezza da adottare per la protezione delle informazioni contenute in documentazione cartacea.

Livello di protezione 1 – basso

Strumenti
Strumenti informatici conformi ai controlli previsti dal Framework Nazionale per la Cybersecurity dell'ACN e alle relative linee guida per le PA, in ottemperanza ai requisiti di resilienza della Direttiva (UE) 2022/2555 (NIS2) e del D.Lgs. 138/2024 - livello minimo.
Portali web e applicazioni senza autenticazione (dati destinati alla divulgazione pubblica), con cifratura delle informazioni in transito mediante protocollo HTTPS/TLS
Supporti rimovibili senza cifratura, limitatamente a dati destinati alla divulgazione pubblica
Backup periodici su infrastruttura gestita dall'amministrazione

Livello di protezione 2 – medio
Oltre alle misure previste dal livello di protezione precedente, si adottano le seguenti.

Strumenti
Strumenti informatici conformi ai controlli previsti dal Framework Nazionale per la Cybersecurity dell'ACN (ex livello standard AgID), in coerenza con le misure NIS2 (D.Lgs. 138/2024).
Portali web e applicazioni con autenticazione, ove tecnicamente possibile a più fattori (MFA), e cifratura delle informazioni in transito (HTTPS/TLS); soluzioni di archiviazione e collaborazione documentale dell'amministrazione con controllo degli accessi (a titolo esemplificativo, ambienti di file sharing/collaborazione quali Active Directory, SharePoint, OneDrive o equivalenti)
Supporti rimovibili con cifratura

Livello di protezione 3 – alto
Oltre alle misure previste dal livello di protezione precedente, si adottano le seguenti.

Strumenti
Strumenti informatici conformi ai controlli previsti dal Framework Nazionale per la Cybersecurity dell'ACN (ex livello avanzato AgID), in coerenza con le misure NIS2 (D.Lgs. 138/2024)
File server cifrato
Backup su infrastruttura centralizzata dell'amministrazione, con verifica periodica del ripristino

Procedure
Accesso ai dati limitato a un elenco nominativo di soggetti autorizzati, con riesame periodico delle autorizzazioni e registrazione (log) degli accessi

Livello di protezione 4 – molto alto
Oltre alle misure previste dal livello di protezione precedente, si adottano le seguenti.

Strumenti
Applicazioni con algoritmi di crittografia forte per le informazioni in transito e basi di dati cifrate
Sistemi operativi installati e mantenuti secondo linee guida di hardening riconosciute (CIS Benchmark o equivalenti)
Sistemi di posta elettronica con cifratura dei messaggi
Il software utilizzato deve avere analisi mensili delle vulnerabilità e aggiornamento continuo
Monitoraggio continuo, registrazione e conservazione degli eventi di sicurezza (log) e segmentazione/segregazione delle reti e degli ambienti che trattano tali dati

5. Livelli di protezione dei dati ed informazioni contenute in documenti cartacei

La protezione dei dati personali contenuti in documentazione cartacea richiede un approccio integrato che, unitamente a un'adeguata formazione del personale in materia di privacy e trattamento dei dati, contempli la preliminare predisposizione di un inventario documentale, il ricorso ad ambienti e arredi idonei a inibire l'accesso ai soggetti non autorizzati e l'adozione di un sistema di tracciamento mediante registro degli accessi, dal quale ricavare le informazioni essenziali sui soggetti autorizzati e sul fascicolo o documento oggetto di consultazione o acquisizione.

La corretta e puntuale combinazione di tali elementi, oltre ad assicurare un'idonea sicurezza nel trattamento delle informazioni, consente una migliore gestione degli incidenti di sicurezza (c.d. *data breach*) — quali, ad esempio, la compromissione di dati personali a seguito di furto, smarrimento o diffusione non autorizzata.

Al fine di prevenire il verificarsi di un *data breach*, è opportuno che le strutture applichino puntualmente le seguenti misure di sicurezza di natura **fisica, organizzativa e procedurale**, volte a limitare gli accessi non autorizzati e a prevenire lo smarrimento o la distruzione accidentale dei dati personali.

Misure fisiche:

archiviazione sicura:

i documenti vanno conservati in mobili contenitori (armadi, cassettiere, ecc.)provvisti di serratura o in ambienti ad accesso limitato e sorvegliatoimpedendo la visione o il furto da parte di persone non autorizzate;

scrivania pulita (Clean Desk Policy):

a tutela della sicurezza delle informazioni riservate (dati personali e dati particolari) e per prevenire accessi non autorizzati, la postazione di lavoro deve essere lasciata completamente sgombra durante le pause, al termine della giornata lavorativa e in occasione di assenze prolungate (ad esempio congedi ordinari o straordinari), avendo cura di riporre i documenti in cassetti o armadietti chiusi a chiave. I documenti cartacei contenenti dati personali non più necessari non devono essere conferiti nei cestini ordinari, ma distrutti mediante distruggidocumenti a norma. L'applicazione di tale prassi, oltre a garantire la conformità al GDPR, promuove un ambiente lavorativo più organizzato e professionale e, ove sia necessario condividere la postazione (*hot desking*), consente un utilizzo più efficiente dello spazio.

tracciabilità:

i movimenti dei fascicoli devono essere sempre registrati mediante appositi registri di carico e scarico, nei quali si dà evidenza dell'identità del soggetto autorizzato, dell'azione eseguita (consultazione, estrazione temporanea del documento) e della data e ora dell'accesso. Tale modalità assicura il rispetto della privacy e la prevenzione di accessi non autorizzati, consentendo il monitoraggio dei soggetti che richiedono, visualizzano o modificano i documenti.

distruzione documentale:

coerentemente con quanto previsto dalla Clean Desk Policy, i documenti cartacei non più necessari devono essere dismessi mediante apparecchiature a norma (distruggidocumenti) che ne consentano il taglio a frammenti.

Misure Organizzative:

classificazione dei documenti:

affinché il trattamento dei dati, soprattutto quelli sensibili, avvenga con la dovuta cura, è necessario assegnare un livello di riservatezza ai documenti oggetto di trattamento per i cui dettagli si rimanda alla tabella esemplificativa dei livelli di protezione contenuta nel presente documento.

Formazione del personale:

il personale deve essere periodicamente istruito sulle buone prassi di gestione documentale: limitare la stampa di documenti superflui, riporre le pratiche in cassetti o armadi chiusi, utilizzare correttamente il titolario di classificazione dipartimentale.

Nomina degli incaricati:

i soggetti autorizzati all'accesso e alla movimentazione dei singoli archivi cartacei devono essere formalmente individuati con apposito atto.

Misure Procedurali:

Gestione dei flussi e scarto:

- limitare, attraverso processi di digitalizzazione, la circolazione di copie cartacee favorendo, ove possibile, l'uso di copie digitali protette da password o cifratura;
- evitare di gettare documenti contenenti dati personali nei normali cestini indifferenziati;
- utilizzare distruggidocumenti con un elevato grado di sicurezza;
- promuovere periodiche iniziative volte all'attivazione di processi di "scarto" dei documenti che hanno perso validità amministrativa e non hanno rilevanza storica. Tale procedura offre molteplici vantaggi quali, ad esempio, l'ottimizzazione degli spazi e l'efficienza operativa riducendo la tempistica di ricerca e recupero dei documenti oggetto di interesse.

6. Esempi di classificazione dei dati

Il responsabile dei dati, o il referente, se nominato, compila una tabella per ogni trattamento dati che deve gestire. Nella tabella elenca i singoli insiemi di dati che costituiscono il trattamento etichettandoli ognuno con un nome, poi barra con una "X" in corrispondenza della corretta tipologia di dati per quell'insieme. Il livello di protezione da applicare all'intero trattamento corrisponde al livello di protezione più alto fra quelli degli insiemi di dati inseriti. Per esempio, la struttura che si occupa della gestione delle risorse umane deve gestire un trattamento con tre insiemi di dati: il primo sono le anagrafiche dei dipendenti con i loro contatti personali, il secondo è costituito dalle eventuali disabilità (fisiche o sensoriali), mentre il terzo l'eventuale partecipazione a associazioni datoriali, sindacali o ordini professionali. Gli insiemi vengono etichettati (Anagrafiche, Disabilità e Giudiziari) e poi viene scelto il tipo di dato corrispondente a ciascun insieme. Siccome il livello di protezione più alto corrisponde all'insieme "Disabilità", il trattamento deve essere gestito con gli strumenti, le procedure e i sistemi di controllo contenuti nel livello di protezione 4 –

molto alto. Si rimanda all'allegato "A" al presente documento per la classificazione dei dati afferenti i trattamenti di competenza dipartimentale

7. Riferimenti

Elenco dei documenti utilizzati e risorse utili per la comprensione o l'approfondimento.

Nome	Contenuti e indirizzi
Regolamento UE 2016/679 (GDPR)	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6264597
"Codice in materia di protezione dei dati personali" D.lgs. 30 giugno 2003, n.196	*https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9042678*
Misure minime di sicurezza ICT	*https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict*
Istruzioni e norme comportamentali vigenti di carattere generale per il trattamento dei dati personali di competenza del Dipartimento regionale dell'Agricoltura	*https://www.regione.sicilia.it/istituzioni/regione/strutture-regionali/assessorato-agricoltura-sviluppo-rurale-pesca-mediterranea/dipartimento-agricoltura/altri-contenuti/privacy-e-sicurezza*
Direttiva (UE) 2022/2555 (NIS2)	https://eur-lex.europa.eu/eli/dir/2022/2555/oj
D.Lgs. 4 settembre 2024, n. 138 (recepimento NIS2)	https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2024-09-04;138
Agenzia per la Cybersicurezza Nazionale (ACN) – Framework Nazionale per la Cybersecurity e misure di sicurezza	https://www.acn.gov.it

Palermo, 09 luglio 2026

Il Titolare del Trattamento
L'Assessore
Luca Sammartino
Firma apposta sulla copia del documento analogico conservato agli atti d'ufficio

Il Responsabile dei trattamenti
Dirigente Generale
Dott. Fulvio Bellomo
Firma apposta sulla copia del documento analogico conservato agli atti d'ufficio