



associazione nazionale dirigenti pubblici  
e alte professionalità della scuola

# PRIVACY KIT COME GESTIRE I DATI CORRETTAMENTE

**Designazione ed istruzioni  
per le strutture territoriali  
di ANP**

**VERSIONE AGGIORNATA  
AL 26.01.2022**

**EUSERVICE**

Data Protection Officer

A CURA DI  
**Angelo Leone  
Diego Dimalta**

# SOMMARIO

---

- PREMESSA
- GLOSSARIO
- DESIGNAZIONE
- POLICY

# PREMESSA

## L'importanza di questo documento.

L'**ANP** Associazione nazionale dei dirigenti pubblici e delle alte professionalità della scuola crede molto nell'importanza della protezione dai dati, in particolar modo quando si tratta dei dati dei propri associati.

Il dato degli iscritti ad ANP è difatti particolarmente sensibile in quanto rivela l'adesione dell'interessato al nostro Sindacato.

La normativa europea (GDPR) prevede particolari cautele nel trattamento di questa tipologia di dati.

ANP provvede direttamente alla raccolta e gestione delle singole iscrizioni, avvalendosi anche delle strutture territoriali **per il tramite dei relativi Presidenti (e di eventuali altri soci da essi individuati) quali soggetti autorizzati e incaricati del trattamento di dati, per le finalità associative nel rispetto dei precisi vincoli delineati nelle pagine seguenti.**

Invitiamo quindi i Presidenti delle strutture territoriali a leggere attentamente il presente documento in quanto in esso sono indicate le esatte modalità con cui potranno trattare i dati in nome e per conto dell'ANP.

Per eventuali domande di chiarimento non esitate a contattarci ai recapiti che troverete in ultima pagina.

Buona lettura.

# GLOSSARIO

## Definizioni ai sensi dell'art. 4 GDPR.

Nelle prossime pagine utilizzeremo una serie di termini mutuati dal Regolamento Europeo sulla Protezione dei Dati (GDPR). Pertanto, al fine di una maggiore comprensione del testo, è opportuno che la lettura sia preceduta dalle seguenti definizioni.

«**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

«**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

«**pseudonimizzazione**»: trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

«**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

# GLOSSARIO

## Definizioni ai sensi dell'art. 4 GDPR.

«**titolare del trattamento**»: persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

«**responsabile del trattamento**»: persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

«**destinatario**»: persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

«**terzo**»: persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

«**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

«**violazione dei dati personali/ "data breach"**»: violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

# DESIGNAZIONE

**A soggetto incaricato del trattamento.**

# A TUTTI I PRESIDENTI

## Designazione a soggetti autorizzati al trattamento.

**Tutti i Presidenti delle sezioni territoriali dell'ANP sono, con il presente documento, designati incaricati del trattamento**, potendo quindi effettuare operazioni di trattamento di dati, comuni e sensibili, riguardanti gli Associati solo a condizione del rispetto delle seguenti indicazioni.

In particolare, con la presente, **l'ANP la autorizza a porre in essere i seguenti trattamenti:**

1. Ricezione, archiviazione, elaborazione e risposta alle richieste pervenute tramite e-mail e social network attraverso i canali ufficiali della struttura territoriale dell'ANP.
2. Raccolta, archiviazione, elaborazione e risposta alle richieste di iscrizione all'ANP pervenute, direttamente sul territorio, da parte di nuovi associati. In tal senso, il Presidente è altresì autorizzato a raccogliere la delega cartacea accompagnata dal documento di identità da inviare alla sede nazionale, anticipandola via e-mail all'indirizzo [iscrizione@anp.it](mailto:iscrizione@anp.it).
3. Ricezione, archiviazione, elaborazione e risposta ad istanze riferibili alle procedure interne dell'ANP come, a titolo esemplificativo, quella per l'elezione degli organi territoriali dell'ANP. In questo caso, previo ottenimento del consenso, sarà possibile per il Presidente pubblicare informazioni ed immagini sul sito istituzionale della struttura territoriale dell'Associazione o su altri canali così come previsto in apposite comunicazioni che saranno trasmesse da ANP.
4. Elaborazione ed invio di newsletter a soggetti per i quali esiste una legittima base giuridica che giustifichi l'invio. Tali newsletter dovranno essere inviate ai soli associati e dovranno riguardare esclusivamente notizie riconducibili alle finalità statutarie.
5. Ricezione dei nominativi aggiornati degli iscritti sul territorio di competenza, con possibilità di estrazione ed archiviazione su supporto cartaceo o digitale per scopi riconducibili all'incarico.

Di contro, **sono assolutamente vietati**, salvo indicazioni scritte in senso opposto da parte del Titolare, i seguenti trattamenti:

- Estrazione di dati dai database dell'ANP, salvo il caso di cui al punto 5 di cui sopra;
- Duplicazioni multiple dei database di ANP, fatte salve le operazioni di backup dei dati.
- Utilizzo di dati forniti dal Titolare per finalità diverse da quelle insite nell'incarico;
- Comunicazione di dati a soggetti non autorizzati;
- Pubblicazione di qualsiasi tipo di dato su internet e, in particolare, sui social network salvo, si ribadisce, istruzioni espresse in senso opposto da parte del Titolare;
- Utilizzo di device in difformità da quanto previsto nella sotto riportata policy BYOD;
- Diffusione di qualsiasi dato sensibile.

Il trattamento dei dati deve avvenire esclusivamente per le finalità che lo statuto ANP delega alle sezioni territoriali. Ogni altra finalità è da ritenersi vietata.

Nell'esercizio delle attività oggetto del Suo incarico o delle Sue mansioni, Le è consentito l'accesso esclusivamente a quei dati strettamente necessari per lo svolgimento dei compiti e mansioni a Lei assegnati e nel pieno rispetto delle indicazioni ricevute.

**Al Presidente, quale unico rappresentante delle strutture locali, è vietato qualificarsi come Titolare del trattamento per le attività riconducibili alla presente nomina e ai documenti tutti che costituiscono il presente documento denominato "Kit Privacy".**

In qualità di incaricato del trattamento dei dati di ANP e dei suoi iscritti, Lei è tenuto a:

1. mantenere il segreto e la massima riservatezza rispetto ai dati personali e non personali di cui potrà venire a conoscenza nell'adempimento del Suo incarico, anche in seguito alla cessazione della Sua carica. In particolare, deve ritenersi riservato ogni dato personale da lei trattato nonché ogni informazione e ogni documento analogico e/o informatico, utilizzati in nome e per conto dell'ANP, per il raggiungimento le finalità dell'ANP medesima. Ogni informazione orale deve sempre essere considerata riservata, così come le informazioni riguardanti terze parti. Quanto alle informazioni da non qualificarsi come informazioni riservate vanno intese tali solo quelle di pubblico dominio, quelle che diventino tali in un momento successivo senza che vi sia violazione del presente accordo di riservatezza ovvero per fatto non imputabile alla parte ricevente.
2. segnalare tempestivamente, e comunque non oltre 10 ore, al Titolare del trattamento (e al Responsabile per la Protezione dei Dati – DPO) eventuali reclami ricevuti da parte dei soggetti interessati al trattamento dei propri dati personali, unitamente a qualunque fatto che a Suo giudizio possa compromettere la sicurezza dei dati trattati;
3. trattare tutti i dati personali di cui viene a conoscenza nell'ambito dello svolgimento delle proprie funzioni in modo lecito, trasparente e secondo correttezza.

Le ricordiamo che la violazione degli obblighi anzidetti comporta conseguenze sia civili sia amministrative.

In caso di violazione delle istruzioni impartite, il Presidente della struttura territoriale sarà responsabile per le conseguenze giuridiche che deriveranno, direttamente o indirettamente, dalla sua condotta attiva od omissiva a titolo di dolo o colpa.

Resta inteso che la nomina quale Incaricato, come prevista e disciplinata nella presente comunicazione, seguirà pedissequamente le sorti della carica sindacale, al cessare della quale cesserà quindi anche l'autorizzazione al trattamento.

Resta, altresì, inteso che nessun compenso o rimborso spetterà al Presidente della struttura territoriale per l'assunzione della funzione di Incaricato di Trattamento dei dati personali di cui al presente atto di nomina.

# POLICY

**Indicazioni pratiche sulla gestione dei  
diversi incombenti.**

# POLICY

## Utilizzo dei sistemi di comunicazione.

In ogni caso, al Presidente della struttura territoriale è richiesto di rispettare scrupolosamente le seguenti indicazioni:

1. Esercitare le mansioni relative alla propria carica solo in luoghi idonei a mantenere la riservatezza dei dati. A tal fine non è consentito raccogliere, archiviare o inviare i dati degli associati, in posti che per la loro conformazione, non consentano un adeguato livello di privacy.
2. E' severamente vietato divulgare i dati degli associati, ad esempio, a mezzo telefono, chat o social media. Quanto al telefono, qualora necessario comunicare alcuni dati ad altri soggetti autorizzati, bisognerà aver cura di non essere ascoltati da terzi, mantenendo sempre un tono di voce moderato.
3. E' obbligatorio utilizzare strumenti dotati di adeguati sistemi di protezione da rischio informatico.
4. E' obbligatorio utilizzare sistemi operativi aggiornati. In tal senso è assolutamente vietato l'utilizzo di sistemi operativi per i quali non sono più rilasciati aggiornamenti di sicurezza da parte del realizzatore del software.
5. E' fatto divieto di utilizzare, per finalità istituzionali, indirizzi e-mail con domini non istituzionali.
6. Sui device ANP è vietato installare qualsiasi programma non strettamente essenziale alla raccolta ed archiviazione dei dati degli iscritti, salvo il ricorso a BYOD disciplinato nella seguente policy.
7. In ogni caso è severamente vietato condividere i nomi ed i dati degli associati con chiunque, compresi possibili partner, in mancanza di una autorizzazione espressa da parte dell'ANP struttura nazionale. Questa previsione non si applica alle comunicazioni tra soggetti autorizzati.
8. E' fatto divieto di archiviare i dati degli iscritti su cloud non istituzionali.

# POLICY

## BYOD, ovvero utilizzo dei propri device.

Con "device" si intende qualsiasi strumento elettronico capace di raccogliere, archiviare e/o trasmettere dati.

Rientrano in questa categoria, a mero titolo esemplificativo, computer, tablet, smartphone, smartwatch, agende elettroniche ecc.

Al Presidente è chiesto di servirsi prioritariamente dei device di proprietà dell'ANP i quali dovranno peraltro essere utilizzati esclusivamente per i fini istituzionali.

Nel caso in cui il Presidente ed i suoi incaricati si servissero di strumenti personali, è richiesto di attenersi alle seguenti indicazioni:

1. In primo luogo, è richiesto il rispetto di tutte quante le indicazioni previste nella POLICY "Utilizzo dei sistemi di comunicazione".
2. Assicurarsi di accedere al sistema operativo con un account riservato all'attività istituzionale e dotato di password sicura. Se si tratta di computer usato da altri, compresi altri membri della famiglia, costoro dovranno connettersi utilizzando un'utenza diversa, anche sul medesimo device.
3. E' vietato utilizzare l'accesso a connessioni Wi-Fi che non richiedano la procedura di verifica e riconoscimento dell'utente.
4. E' possibile collegarsi ai soli dispositivi mobili (es. pen drive e hard disk esterni) di cui si conosce la provenienza.
5. Si consiglia di allestire la postazione di lavoro in modo da garantire la riservatezza dei dati ed effettuare il log-out dai servizi/portali utilizzati dopo che è stata conclusa la sessione lavorativa.
6. Implementare sistemi di backup, prediligendo servizi cloud o dispositivi di archiviazione cifrati (es. pen drive e hard disk esterni).

# POLICY

## Sito internet della struttura territoriale.

Al Presidente della struttura territoriale è concessa la creazione di un sito della struttura territoriale. Indipendentemente dalla proprietà del sito, la Titolarità del trattamento rimarrà in capo alla struttura nazionale di ANP. E' quindi fatto divieto alle strutture locali di autoproclamarsi Titolari del trattamento per le attività di cui al sito internet.

Inoltre, al Presidente è richiesto di attenersi scrupolosamente alle seguenti indicazioni:

1. Il sito deve essere allocato su server in unione europea.
2. Il sito non deve contenere alcun cookie analitico, marketing o di profilazione. Sono concessi i soli cookie tecnici di sessione.
3. Il sito non può contenere form privi del rimando all'informativa e, ove necessario, della richiesta di adeguato consenso.
4. Sul sito non devono essere promossi eventi diversi da quelli riconducibili alle finalità statutarie.
5. Sul sito non devono essere pubblicate foto senza prima richiedere gli opportuni consensi.
6. Per la creazione di eventuali newsletter è necessario che le stesse siano pensate in modo da garantire la presenza di idonea informativa e la raccolta dei necessari consensi, con particolare attenzione alla possibilità di richiedere in qualsiasi momento la cancellazione dall'elenco degli iscritti alla newsletter stessa.

# POLICY

## Data Breach.

Un data breach è una violazione della sicurezza che comporta accidentalmente o illegalmente - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali, trasmessi, archiviati o altrimenti elaborati.

**In caso di violazione ANP ha solo 72 ore per notificare l'avvenuto al Garante privacy. Per questo motivo il Presidente della struttura territoriale, in caso di data breach è tenuto a comunicare l'avvenuto entro e non oltre 10 ore dalla conoscenza del fatto.**

### Tipi di violazione dei dati

Di seguito sono elencati alcuni casi tipici di violazione dei dati:

- Furto di credenziali di autenticazione a seguito di un attacco di phishing
- Perdita di una chiavetta USB o di un telefono cellulare o laptop con conseguente perdita di documenti contenenti dati personali
- Cancellazione accidentale o pubblicazione indesiderata di un database su Internet
- Accesso a informazioni riservate da parte di utenti non autorizzati

### Come gestire una violazione dei dati?

#### **Valutazione e contenimento: primi 10 minuti dalla conoscenza del fatto**

In caso di incidente di sicurezza (accertato o sospetto), il Presidente della struttura territoriale deve procedere come segue:

1. Chiamare immediatamente la struttura nazionale di ANP la quale contatterà il DPO.
2. Interrompere la perdita di dati aggiuntivi: portare offline le macchine interessate, ma non disattivarle. Disattivare quindi il Wi-Fi o scollegare il cavo Ethernet dal laptop.
3. Registrare il momento della scoperta: inviare una mail a [segreteria@anp.it](mailto:segreteria@anp.it) e in copia a [rpd@euservice.it](mailto:rpd@euservice.it) con le seguenti informazioni: chi ha scoperto la violazione, chi l'ha segnalata, a chi è stata segnalata, chi altro ne è a conoscenza e che tipo di violazione si è verificata.

#### **Report: i successivi 20 minuti dalla conoscenza del fatto.**

Il soggetto (o i soggetti) che ha scoperto la violazione dei dati personali deve poi annotare:

- il dispositivo interessato, nonché la causa e l'entità;
- le categorie e il numero approssimativo di persone interessate;
- le categorie e il volume approssimativo di dati personali interessati;
- una descrizione delle possibili conseguenze della violazione dei dati personali.

Un'e-mail con le informazioni di cui sopra deve essere inviata immediatamente a [segreteria@anp.it](mailto:segreteria@anp.it) e in copia a [rpd@euservice.it](mailto:rpd@euservice.it)

# **PRIVACY KIT COME GESTIRE I DATI CORRETTAMENTE**

**Designazione ed istruzioni  
per le tutte strutture  
territoriali di ANP**



**VERSIONE AGGIORNATA  
AL 26.01.2022**