REGOLAMENTO

VIOLAZIONI DEI DATI PERSONALI - DATA BREACH

AUTOMOBILE CLUB D'ITALIA

INDICE

REGOLAMENTO

VIOLAZIONI DEI DATI PERSONALI - DATA BREACH

TITOLO I

CAPO I

DISPOSIZIONI GENERALI

CAPO II

SISTEMA DI PREVENZIONE DEI RISCHI

CAPO III

IDENTIFICAZIONE E GESTIONE DELLE VIOLAZIONI - DATA BREACH

Capo IV

NOTIFICA ALL'AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI E COMUNICAZIONE AGLI INTERESSATI

Capo V

MISURE DA ADOTTARE E MIGLIORAMENTO CONTINUO

o o o o o

TITOLO I

CAPO I
DISPOSIZIONI GENERALI

Art. 1
Finalità

1. Il presente regolamento stabilisce le responsabilità e le procedure operative ai fini della gestione delle violazioni dei dati personali (*data breach*) in ACI, in conformità al Regolamento UE 2016/679 (di seguito, GDPR) e alle vigenti disposizioni nazionali e comunitarie. Esso mira a garantire che ogni violazione venga trattata in modo tempestivo ed efficace, minimizzando i rischi per i diritti e per le libertà degli interessati e garantendo la conformità (*compliance*) normativa ed operativa.

2. Le *policy* interne di gestione delle violazioni dei dati costituiscono una componente essenziale in termini di data governance.

Art. 2
Ambito di applicazione

1. Il presente regolamento si applica alle Strutture centrali e territoriali dell'ACI, relativamente ai trattamenti di dati personali dei quali l'ACI sia titolare, contitolare o responsabile ai sensi delle disposizioni di cui Capo IV del GDPR e riguarda tutte le attività di trattamento dei dati personali, inclusi i dati particolari e i dati giudiziari, effettuate dall'ACI e comprese quelle gestite da terze parti in qualità di responsabili esterni del trattamento ai sensi dell'art. 28 del GDPR.

Art. 3
Indirizzi per gli Automobile Club e per le Società controllate

1. Il presente regolamento costituisce un atto di indirizzo per i singoli Automobile Club provinciali e locali federati, in considerazione del vincolo federativo e della coincidenza del Data Protection Officer (di seguito, DPO) di ACI con il DPO dei singoli Automobile Club. Le società controllate dall'ACI ai sensi del Testo unico in materia di società a partecipazione pubblica (decreto legislativo 9 agosto 2016, n. 175 e s.m.i.) ne terranno conto ai fini dell'adozione dei propri Regolamenti. Resta ferma la necessità, in funzione di *governance* e di *compliance* complessiva, che ogni Automobile Club e ogni società controllata adotti un proprio Regolamento in materia di *data breach*.

Art. 4
Definizioni

1. Per "**dato personale**" si intende "*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*" (art. 4, paragrafo 1 del GDPR).

2. Per "**trattamento**" si intende "*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*" (art. 4, paragrafo 2 del GDPR).

3. Per "**violazione dei dati personali**" (***data breach***) si intende "*la 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*" (art. 4 paragrafo 12 del GDPR).

4. Per la "**sicurezza del trattamento**", l'art. 32 del GDPR prevede che il Titolare e il Responsabile ex art. 28 GDPR adottino misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, fra le altre, se del caso: *"a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento*".

5. Per "**Responsabile della Protezione Dati**" (Data Protection Officer - DPO), ai sensi degli artt.37 e 38 del GDPR si intende il dipendente del titolare (o del responsabile del trattamento) oppure il soggetto che assume tale incarico in base ad un contratto di servizi, designato in funzione delle qualità professionali e della capacità di assolvere i compiti indicati nell'art.39 del GDPR.

6. Per "**Comitato di crisi**" si intende l'Organismo interno istituito per fronteggiare tempestivamente situazioni che comportino rischi e minacce per la gestione dei dati personali. Il Comitato è coordinato dal Titolare anche per il tramite del Segretario Generale.

7. Per "***compliance***" si intendono la predisposizione e l'attuazione delle misure tecniche ed organizzative atte a garantire la conformità delle operazioni di trattamento alla normativa esercitate attraverso le attribuzioni e le condotte dei Referenti, da adottarsi, in chiave preventiva dei rischi, con il supporto della Struttura di *compliance* Direzione Organizzazione e Gestione della Privacy e Monitoraggio del Sistema di Qualità dell'Ente (di seguito, DPQ), in accordo con il DPO.

CAPO II
SISTEMA DI PREVENZIONE DEI RISCHI

Art. 5
Misure da adottare

1. L'ACI adotta misure tecniche e organizzative adeguate a garantire un livello di sicurezza appropriato ai rischi, inclusi i controlli di accesso, crittografia, e il monitoraggio delle attività di sistema, in linea con gli artt.5, paragrafo 1, lettera f) e 32 del GDPR (Considerando 83 e 84).

2. In relazione a ciascun trattamento e, in particolare, preliminarmente all'introduzione di nuovi processi o tecnologie che potrebbero comportare un alto rischio per i diritti e le libertà degli interessati, deve essere condotta una valutazione d'impatto sulla protezione dei dati (DPIA) per identificare e mitigare i rischi potenziali, così come previsto dall'art. 35 del GDPR (Considerando da 89 a 95).

3. L'ACI prevede programmi di formazione e sensibilizzazione periodici per tutti i dipendenti e fornisce indicazioni incentrate sul corretto trattamento dei dati, sulle responsabilità individuali e sulle procedure di gestione di eventuali violazioni dei dati personali.

4. Sessioni periodiche di aggiornamento devono essere tenute, in particolare, in relazione a modifiche normative e in caso di significative violazioni di dati, per assicurare che tutto il Personale sia al corrente delle procedure e delle misure di sicurezza adottate.

Capo III

IDENTIFICAZIONE E GESTIONE DELLE VIOLAZIONI - DATA BREACH

Art. 6
Data breach - Definizione e classificazioni

1. Per "***data breach***" si intende un evento qualsiasi che determini una violazione dei dati personali di cui all'art. 4, paragrafo 12 del GDPR. Una violazione dei dati personali può compromettere, anche contemporaneamente, la riservatezza, l'integrità, la disponibilità dei dati personali, nonché qualsiasi combinazione di questi elementi.

2. Secondo le vigenti linee guida dell'European Data Protection Board (di seguito, EDPB) 9/2022 sulla notifica della violazione di dati personali tali violazioni possono essere classificate in tre macro categorie:

A. **violazione della riservatezza,** in caso di divulgazione o di accesso non autorizzato o accidentale ai dati personali. A titolo esemplificativo e non esaustivo si includono l'invio erroneo di dati personali appartenenti alla categoria di dati particolari, la divulgazione di dati personali al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento, l'accesso non autorizzato da parte di un dipendente o un attacco informatico che consente l'accesso ai dati personali, oppure la connessione, senza sforzo irragionevole, di dati ad altre informazioni che consentano l'individuazione dell'interessato, oppure l'utilizzo dei dati per finalità diverse da quelle previste o in modo non lecito;
B. **violazione dell'integrità,** in caso di modifica non autorizzata o accidentale dei dati personali (come, ad esempio, l'alterazione di record o la modifica di dati);
C. **violazione della disponibilità,** in caso di perdita o di distruzione accidentale o non autorizzata dei dati personali. A titolo esemplificativo e non esaustivo si ricomprendono l'eliminazione accidentale di file critici, la perdita di dati causati da un attacco *ransomware* o la perdita di chiavi di crittografia.

Art. 7
Identificazione e segnalazione interna della violazione

1. L'ACI, attraverso la Direzione per lo Sviluppo, la Gestione, la Sicurezza dei Sistemi Informativi e l'Innovazione Digitale, ha adottato un sistema di controllo per rilevare tempestivamente anomalie, accessi non autorizzati e altre attività sospette che potrebbero comportare una violazione dei dati personali.

2. Chiunque, dipendente, collaboratore di ACI, responsabile esterno, soggetto terzo, rilevi o sospetti una violazione di dati deve segnalarla senza ritardo al Titolare e per opportuna conoscenza al DPO di ACI con email agli indirizzi di posta privacy@aci.it e m.annibalidpo@aci.it.

3. Ogni incidente segnalato che determina una violazione dei dati personali deve essere, senza ritardo, registrato e documentato nell'allegato schema di "Registro delle Violazioni", in linea con l'art.33, paragrafo 5 del GDPR, includendo, tra l'altro, la data e l'ora della segnalazione, il tipo di incidente, i dati coinvolti e le azioni iniziali intraprese. Il Registro è detenuto dalla Struttura di *compliance* dell'Ente (DPQ).

4. Il Registro deve essere costantemente aggiornato con le violazioni occorse e mantenuto in sicurezza. È fatto obbligo di registrare in modo tempestivo ed accurato i dettagli di ogni violazione.

5. Qualora l'incidente non comporti una violazione che determini un rischio significativo per i diritti e per le libertà degli interessati, lo stesso sarà documentato

puntualmente dalla Struttura che ha rilevato l'incidente e sarà oggetto di una segnalazione al Titolare da inviare all'indirizzo di posta privacy@aci.it e per opportuna conoscenza al DPO all'indirizzo m.annibalidpo@aci.it. Le Strutture interessate valuteranno le misure tecniche ed organizzative da adottare per minimizzare i rischi nel trattamento dei dati personali.

6. Alla casella cybersecurity@aci.it vengono segnalati unicamente i tentativi sospetti di accesso indebito che non abbiano originato ancora un'eventuale *data breach*.

Art. 8
Contenimento del rischio e recupero dei dati compromessi

1. Il Comitato di crisi è l'Organismo interno istituito per fronteggiare tempestivamente situazioni che comportino rischi e minacce per la gestione dei dati personali.

2. Il Comitato opera secondo il disciplinare di funzionamento da adottarsi entro 30 giorni dalla data di vigenza del presente Regolamento.

3. Il Comitato opera con le Strutture di competenza coinvolte, in collaborazione con i responsabili della sicurezza fisica e informatica. Adotta misure tecniche ed organizzative immediate per limitare l'estensione della violazione (contenimento del rischio) quali, a titolo esemplificativo e non esaustivo, la sospensione degli *account* utente compromessi, il blocco degli accessi non autorizzati.

4. Il recupero dei dati compromessi deve essere eseguito tempestivamente, cercando di ripristinare i dati allo stato originario precedente alla violazione. Il Titolare, per il tramite delle Strutture di competenza coinvolte, adotta e documenta le misure di sicurezza necessarie.

5. Dopo aver contenuto l'incidente, limitandone gli effetti ove possibile, sarà condotta un'analisi approfondita per valutare l'origine della violazione, identificare eventuali vulnerabilità e determinare se l'incidente è stato completamente risolto, al fine di adottare misure necessarie per evitare che l'incidente di sicurezza possa ripetersi.

6. Sono componenti permanenti del Comitato di crisi i Rappresentanti delle seguenti Funzioni organizzative dell'Ente:
- Presidenza e Segreteria Generale
- Sistemi Informativi
- Data Protection Officer (DPO)
- Privacy Compliance
- Avvocatura
- Risorse Umane
- Comunicazione.

Il Comitato è presieduto dal Titolare anche per il tramite del Segretario Generale, in ogni caso componente permanente del Comitato, e viene, di volta in volta, integrato dagli Owner dei processi oggetto degli incidenti di sicurezza e dai Rappresentanti delle società collegate ACI interessati dagli stessi Owner.

7. La Direzione Organizzazione e Gestione della Privacy e Monitoraggio del Sistema di Qualità dell'Ente è incaricata di provvedere alla formalizzazione delle nomine dei Componenti designati per il Comitato di crisi.

Art. 9
Valutazione del rischio e analisi delle conseguenze

1. Una volta contenuta la violazione, il DPO di ACI coordina una valutazione del rischio per determinarne l'entità e le conseguenze, inclusi i possibili effetti a lungo termine del danno concreto e potenziale per i diritti e per le libertà degli interessati. Questa valutazione deve considerare la tipologia e il volume dei dati compromessi, inclusi gli eventuali dati particolari, o relativi a condanne penali e reati, il numero e le categorie dei soggetti interessati, le possibili conseguenze per gli individui.

2. La valutazione del rischio viene effettuata utilizzando strumenti standardizzati, come l'allegato diagramma di flusso operativo fornito dall'EDPB nelle citate linee guida e include la classificazione della gravità dell'incidente.

Capo IV
NOTIFICA ALL'AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI E COMUNICAZIONE AGLI INTERESSATI

Art. 10
Notifica all'Autorità Garante per la protezione dei dati personali

1. L'art. 33 del GDPR stabilisce che: "*In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente a norma dell'art. 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo*".

2. In linea con il disposto dell'art. 33 del GDPR (Considerando 85, 87, 88), in caso di violazione che comporti un rischio per i diritti e le libertà degli interessati, le violazioni da notificare sono quelle che possono produrre effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali.

3. Al fine di valutare se la violazione occorsa possa presentare un rischio per i diritti e le libertà degli interessati, ci si avvale dello strumento di autovalutazione disponibile sul sito del Garante per la protezione dei dati personali.

4. L'istruttoria finalizzata alla notifica avviene da parte del Comitato di crisi con la collaborazione delle Strutture coinvolte.

5. La notifica deve essere inviata all'Autorità Garante entro 72 (settantadue) ore dalla conoscenza della violazione. Deve includere una descrizione dettagliata della violazione, delle sue conseguenze e delle misure adottate per mitigarne gli effetti. La notifica deve contenere elementi essenziali quali: la natura della violazione dei dati personali, compreso il tipo e il volume dei dati compromessi; le categorie e il numero anche approssimativo di interessati; i dati di contatto del DPO o di altro punto di contatto; le probabili conseguenze della violazione; le misure adottate o proposte per affrontare la violazione e attenuare i possibili effetti negativi.

6. La notifica all'Autorità Garante, effettuata dal Titolare per il tramite della Struttura di *compliance* (DPQ), viene inviata attraverso un'apposita procedura informatica disponibile sul sito istituzionale dell'Autorità.

7. La notifica viene definita dal Garante per la protezione dei dati personali come "completa" quando si hanno tutti gli elementi identificativi della fattispecie verificatasi, con le misure di attenuazione del rischio definite. La notifica viene contraddistinta come "preliminare" quando non sono ancora disponibili tutte le informazioni: in tal caso, il Titolare del trattamento riceverà messaggi dal Garante per la protezione dei dati personali per completare le necessarie informazioni.

Art. 11
Comunicazione agli interessati

1. Come previsto dall'art. 34 del GDPR, se la violazione comporta un rischio elevato per i diritti e le libertà degli interessati, questi devono essere informati senza ingiustificato ritardo.

2. La comunicazione deve essere chiara, concisa e facilmente comprensibile e deve includere: la descrizione della natura della violazione dei dati personali; il nome e i dettagli di contatto del DPO o di altro punto di contatto da cui ottenere ulteriori informazioni; le probabili conseguenze della violazione; le misure adottate o proposte per affrontare la violazione e mitigarne gli effetti, inclusi eventuali consigli agli interessati per tutelarsi. Può essere effettuata tramite i canali ritenuti più appropriati (come e-mail, posta o comunicazione diretta) a seconda della gravità della violazione e delle circostanze specifiche.

3. La comunicazione agli interessati non è necessaria se è soddisfatta una delle seguenti condizioni:

- il Titolare del trattamento ha applicato misure tecniche e organizzative (come, a titolo indicativo e non esaustivo, la cifratura) adeguate ai dati personali oggetto della violazione;
- sono state adottate successivamente misure per evitare che si concretizzi un elevato rischio per i diritti e le libertà degli interessati;
- qualora la comunicazione all'interessato richieda sforzi sproporzionati (in tal caso, si procederà a una comunicazione pubblica o misura simile).

Capo V
MISURE DA ADOTTARE E MIGLIORAMENTO CONTINUO

Art. 12
Piano di risposta agli incidenti (*Remediation plan*)

1. L'ACI redige un Piano di risposta agli incidenti (cd. *remediation plan*) predisposto dal Comitato di crisi che definisce le procedure specifiche da seguire in caso di violazione dei dati, per ripristinare la normale operatività il più rapidamente possibile, minimizzando i tempi di inattività e riducendo il più possibile l'impatto sugli interessati. In tale Piano vengono definiti i ruoli e le responsabilità del Personale coinvolto per garantire la continuità operativa.

2. Il Piano di risposta agli incidenti deve essere periodicamente testato, attraverso simulazioni ed esercitazioni pratiche, per assicurare che il Personale sappia rispondere efficacemente ad una eventuale violazione dei dati.

Art. 13
Verifica post incidente e miglioramento continuo

1. Dopo la definizione dell'incidente da cui è scaturita una violazione dei dati, il DPO conduce una verifica a posteriori per valutare l'efficacia della risposta adottata, l'adeguatezza delle misure preventive esistenti e per identificare eventuali lacune nei sistemi di sicurezza, informandone il Comitato di crisi per l'adozione delle conseguenti misure.

2. Di dette attività il DPO redige un rapporto per il Titolare, includendo una sintesi dell'incidente, le cause identificabili, le azioni correttive adottate e le raccomandazioni per prevenire future violazioni.

3. In base ai risultati della verifica post incidente, le politiche e le procedure interne devono essere aggiornate per affrontare eventuali vulnerabilità scoperte e per migliorare la gestione dei trattamenti dei dati personali.

4. Oltre alla verifica post incidente, vengono effettuate valutazioni periodiche da parte delle Strutture interessate e deputate alle politiche di sicurezza dei dati e della

gestione di eventuali violazioni, in modo da assicurare un continuo miglioramento delle misure da adottarsi.

Articolo 14
Norma di chiusura

1. Il presente Regolamento sarà sottoposto a revisione periodica in occasione di modifiche normative o organizzative sostanziali, per garantirne la costante adeguatezza rispetto all'evoluzione della normativa ed alle esigenze operative dell'ACI.

All. Schema di Registro delle Violazioni (Data Breach ex art.33, c.5 del Regolamento UE 2016/679 - GDPR)

REGISTRO DELLE VIOLAZIONI (DATA BREACH ex art. 33, c.5 del Regolamento UE 2016/679 – GDPR)			
ENTE TITOLARE DEL TRATTAMENTO		**Responsabile protezione dei dati**	
indirizzo		indirizzo	
n. telefono		n. telefono	
mail		mail	
PEC		PEC	
Delegato del titolare (eventuale)		**Registro tenuto da**	
indirizzo		data creazione	
n. telefono		ultimo aggiornamento	
mail		n. schede compilate	
PEC		prossima revisione	
n. ordine			
Luogo, data e ora			
Modalità con cui ACI è venuto a conoscenza della violazione (rilevazione da parte del titolare; comunicazione da parte del responsabile del trattamento; segnalazione da parte di interessato o soggetto terzo; notizie stampa; altro)			
Momento in cui il titolare è venuto a conoscenza della violazione (data e ora)			
Motivi del ritardo (in caso di notifica oltre le 72 ore)			
Soggetti coinvolti nel trattamento (Contitolare, Responsabile del trattamento, etc.)			
Natura della violazione (perdita di: a) riservatezza, b) integrità, c) disponibilità)			
Causa della violazione (azione intenzionale interna o esterna; azione accidentale interna o esterna; sconosciuta)			
Descrizione della violazione			
Descrizione dei sistemi, sw, servizi e infrastrutture IT coinvolti, con indicazione della loro ubicazione			
Misure tecniche e organizzative in essere al momento della rilevazione			

Categorie di interessati (dipendenti, soci, utenti, minori, contraenti, soggetti che ricoprono cariche sociali, etc.)	
Numero (anche approssimativo) di interessati coinvolti (o, in alternativa, se al momento non è determinabile o non ancora determinato)	
Categorie di dati personali violati (dati anagrafici: nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale; dati di contatto: indirizzo postale o di posta elettronica, numero di telefono fisso o mobile; dati di accesso e di identificazione: username, password, customer ID, altro:…; dati di pagamento: numero di conto corrente, dettagli della carta di credito, altro…; dati particolari (specificando di quale si tratti: relativi alla salute, all'appartenenza sindacale, etc; dati relativi a condanne penali e ai reati o a connesse misure di sicurezza; dati di profilazione; dati relativi a documenti di identificazione/di riconoscimento, dati relativi all'ubicazione; altro: ....)	
Numero (anche approssimativo, non determinato o ancora non determinabile) di registrazioni di dati personali (es. record di database, n. fatture, n. transazioni)	
Dettaglio delle categorie di dati personali oggetto della violazione per ciascuna categoria di interessati (aggiungere allegato di riferimento ove necessario)	
Probabili conseguenze in caso di perdita di riservatezza: a) i dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento; b) i dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati; c) i dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito; d) altro	
Probabili conseguenze in caso di perdita di integrità: a) i dati sono stati modificati e resi inconsistenti; b) i dati sono stati modificati mantenendo la consistenza; c) altro	
Probabili conseguenze in caso di perdita di disponibilità: a) mancato accesso a servizi; b) malfunzionamento e difficoltà nell'utilizzo di servizi; c) altro: impossibilità di accesso o distruzione non autorizzata o accidentale, etc.	

Ulteriori considerazioni sulle probabili conseguenze	
Potenziale impatto per gli interessati (perdita del controllo dei dati personali, limitazioni dei diritti, frodi, perdita dati protetti da segreto professionale, conoscenza da parte di terzi non autorizzati, danno economico o sociale significativo, altro...)	
Gravità del potenziale impatto sugli interessati (trascurabile, bassa, media, alta, non definita)	
Misure tecniche e organizzative adottate (o proposte) per porre rimedio o limitare gli effetti negativi per gli interessati)	
Misure tecniche e organizzative adottate (o proposte) per prevenire simili violazioni future	
Notifica (se sì, indicare Garante Privacy ed eventualmente altri Organismi di vigilanza o controllo)	
Motivare la notifica e/o la mancata notifica o il ritardo nella notifica	
Tipo di notifica (preliminare, completa, integrativa)	
Segnalazione all'Autorità Giudiziaria o di Polizia	
La violazione è suscettibile o meno di presentare un rischio elevato per i diritti e le libertà delle persone fisiche	
Comunicazione agli interessati (se sì, indicare le modalità)	
Motivare la mancata comunicazione della violazione agli interessati	
Parere del DPO	
Altro	

All.Diagramma di flusso dell'EDPB con i requisiti di notifica all'Autorità Garante

A. Diagramma di flusso che mostra i requisiti di notifica