Palazzo Cesaroni
Piazza Italia, 2
06121 PERUGIA

XI LEGISLATURA

ALLEGATO A
AL PROCESSO VERBALE DELL'UFFICIO DI PRESIDENZA

DELIBERAZIONE N. 20 DEL 21 MARZO 2022

OGGETTO N. 04 **REGOLAMENTO PRIVACY UE 2016/679 - GDPR- Procedura per la notifica di una violazione dei Dati Personali "Data Breach" ai sensi dell'art. 33 del GDPR e dell'art. 26 del D.lgs 51/2018.**

Marco Squarta	*Presidente*	X	
Michele Bettarelli	*Vice Presidente*	X	
Paola Fioroni	*Vice Presidente*	X	

PRESIDENTE: Marco Squarta

SEGRETARIO VERBALIZZANTE: Juri Rosi

Palazzo Cesaroni
Piazza Italia, 2
06121 PERUGIA

L'UFFICIO DI PRESIDENZA

VISTA la legge regionale 12 giugno 2007, n. 21 (Struttura organizzativa e dirigenza del Consiglio regionale) e successive modificazioni;

VISTA la deliberazione dell'Ufficio di presidenza n. 156 dell'11 settembre 2007 (Approvazione del 'Regolamento di organizzazione della struttura organizzativa e della dirigenza del Consiglio regionale', ai sensi dell'art. 2 della legge regionale 12 giugno 2007, n. 21), come modificata dalle deliberazioni n. 243 del 13 marzo 2008, n. 102 del 30 dicembre 2010, n. 391 del 19 novembre 2018, n. 1 del 11 gennaio 2019 e n. 101 del 20 dicembre 2019;

VISTA la deliberazione dell'Ufficio di Presidenza 18 giugno 2018, n. 358 (Regolamento di disciplina del funzionamento dell'Ufficio di Presidenza, della formazione e della adozione degli atti amministrativi di competenza del Presidente dell'Assemblea legislativa, dell'Ufficio di presidenza, del Segretario generale e dei dirigenti della Segreteria generale dell'Assemblea legislativa), come modificato dalla deliberazione dell'UP n.61/2021 e in particolare l'articolo 10;

ESAMINATA la proposta di deliberazione ordinaria trasmessa dal Segretario generale ai sensi del citato art. 10 del regolamento e allegata al presente atto;

PRESO ATTO del parere di regolarità amministrativa e dell'attestazione di irrilevanza del parere di regolarità contabile;

RITENUTO di accogliere la proposta di deliberazione in argomento per le motivazioni in fatto e diritto nella stessa riportate;

con voti unanimi espressi nei modi di legge

D E L I B E R A

1)-**Di approvare** la Procedura per la notifica di una violazione dei Dati Personali "Data Breach" ai sensi dell'art. 33 del Reg. Ue n. 679/2016 e dell'art. 26 del D.lgs 51/2018 di cui all'**allegato A** che costituisce parte integrante e sostanziale del presente atto;

2)-**Di disporre** che sono sottoposti all'osservanza della Procedura di cui al punto che precede tutti coloro che sono autorizzati al trattamento di dati personali (personale dipendente dell'Assemblea legislativa, personale dipendente e collaboratori dei Gruppi consiliari, i Consiglieri regionali, gli Assessori regionali non Consiglieri);

4)-**Di dare atto** che dal presente atto non derivano spese o oneri aggiuntivi per l'Assemblea legislativa;

5)-**Di dare atto** che il presente atto è soggetto a pubblicazione nel sito istituzionale ai sensi dell'art. 12 del d.lgs. n.33/2013;

6)-Di disporre che il presente atto e l'unito allegato siano pubblicati a cura del responsabile della Sezione Segreteria di direzione, cerimoniale ed educazione alla cittadinanza nel sito istituzionale Sezione amministrazione trasparente nella pagina https://trasparenza.alumbria.it/atti-amministrativi-generali e nella pagina https://trasparenza.alumbria.it/provvedimenti-organi-indirizzo-politico a mezzo collegamento (link) alla prima pubblicazione;

7)-**Di trasmettere** il presente atto e l'unito allegato al RPD interno, al Segretario generale, ai dirigenti, ai componenti della Rete dei referenti privacy, al responsabile della posizione Sezione sistema informatico, ciascuno per il seguito di competenza;

8)-**Di trasmettere** il presente atto e l'unito allegato al personale dipendente dell'Assemblea legislativa, al personale dipendente e ai collaboratori dei Gruppi consiliari, ai Consiglieri regionali, agli Assessori regionali non Consiglieri, al Presidente del Corecom, al Presidente dell'ISUC, al Presidente del CSGP, all'Ufficio di presidenza del CAL, al Difensore civico regionale.

Il Segretario Verbalizzante
Juri Rosi

Il Presidente
Marco Squarta

Palazzo Cesaroni
Piazza Italia, 2
06121 PERUGIA

REGOLAMENTO PRIVACY UE 2016/679 - GDPR- Procedura per la notifica di una violazione dei Dati Personali "Data Breach" ai sensi dell'art. 33 del GDPR e dell'art. 26 del D.lgs 51/2018.

PROPOSTA DI DELIBERAZIONE DELL'UFFICIO DI PRESIDENZA

VISTA la legge regionale 12 giugno 2007, n. 21 (Struttura organizzativa e dirigenza del Consiglio regionale);

RICHIAMATO il Codice dell'Amministrazione Digitale, D.Lgs. n. 82/2005, così come modificato dal D.Lgs. n. 179/2016, che all'art. 51, rubricato "Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni", prevede che "i documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta";

RICHIAMATO il Regolamento Europeo Privacy UE/2016/679 (di seguito GDPR) che stabilisce le nuove norme in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché le norme relative alla libera circolazione di tali dati ed introduce nel nostro ordinamento giuridico il "principio di accountability" (obbligo di responsabilizzazione) che impone alle Pubbliche Amministrazioni titolari del trattamento dei dati:
-di dimostrare di avere adottato le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche;
-che i trattamenti siano conformi ai principi e alle disposizioni del Regolamento, prevedendo, altresì, l'obbligo del titolare o del responsabile del trattamento della tenuta di apposito registro delle attività di trattamento, compresa la descrizione circa l'efficacia delle misure di sicurezza adottate;

RICHIAMATE in particolare le seguenti disposizioni del citato GDPR:
-l'art.5, lett.f) il quale impone che i dati personali siano trattati in maniera da garantire un'adeguata sicurezza dei dati personali medesimi, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»);
-l'art.4, punto n.12) il quale prevede che per "Violazione di dati" 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;
-l'art.33 il quale, tra l'altro, prevede che in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente senza ingiu-

stificato ritardo, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche e che il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio;
-l'art.34 il quale, tra l'altro, prevede che quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo;

VISTO l'art.26 del decreto legislativo 18 maggio 2018, n. 51 ("Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio");

VISTE le Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679 del 3 ottobre 2017, versione emendata ed adottata il 6 febbraio 2018 dal Gruppo di lavoro articolo 29 per la protezione dei dati (WP250rev.01), fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018;

VISTO il provvedimento del 27 maggio 2021 dell'Autorità Garante per la protezione dei dati con il quale è stata adottata un'apposita procedura telematica che i titolari del trattamento devono utilizzare, a far data dal 1 luglio 2021, per la notifica delle violazioni;

VISTO il Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) 2016/679 (d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101, di seguito "Codice");

DATO ATTO che ai sensi dell'art.4, punto n.7) del citato GDPR l'Assemblea legislativa è il Titolare del trattamento dei dati personali (di seguito "il Titolare");

RICHIAMATA la propria deliberazione n.85 del 27 luglio 2020 avente ad oggetto "Regolamento privacy UE 2016/679 – General Data Protection Regulation (GDPR) – Definizione dell'assetto organizzativo– Approvazione del registro dei trattamenti, di accountability e delle violazioni - Avvio delle attività di compliance normativa";

PRESO ATTO che in data 1 marzo 2022 è cessato l'incarico di RPD affidato alla Fondazione LogosPA e che con provvedimento n.35 del 1 marzo 2022 il Segretario generale, in qualità di delegato del Titolare, ha nominato RPD interno la dipendente Sabrina Di Cola, già referente generale privacy;

TENUTO CONTO che al fine della corretta e tempestiva gestione delle violazioni dai dati personali il precedente RPD Fondazione LogosPA, in accordo con il Segretario

generale e la referente generale della privacy, ha predisposto la procedura per la notifica di una violazione dei Dati Personali "Data Breach" di cui all'allegato A;

RITENUTO che la procedura per la notifica di una violazione dei Dati Personali "Data Breach" di cui all'allegato A sia a garanzia del puntuale adempimento di quanto previsto dall'art.33 del GDPR e dall'art.26 del D.lgs 51/2018;

RITENUTO necessario precisare che la procedura per la notifica di una violazione dei Dati Personali "Data Breach" di cui all'allegato A deve essere osservata da tutti coloro che sono autorizzati al trattamento di dati personali (personale dipendente dell'Assemblea legislativa, personale dipendenti e collaboratori dei Gruppi consiliari, i Consiglieri regionali, gli Assessori regionali non Consiglieri);

CONSIDERATO che la procedura per la notifica di una violazione dei Dati Personali "Data Breach" è un atto amministrativo generale e quindi è soggetto a pubblicazione nel sito istituzionale ai sensi dell'art.12 del d.lgs. n.33/2013;

TENUTO CONTO che con provvedimento del Segretario generale n.95 del 16 agosto 2021 (prot.n.5180/2021) il Responsabile della Sezione Segreteria di direzione, cerimoniale ed educazione alla cittadinanza è il referente della pubblicazione sia degli atti amministrativi generali che dei provvedimenti dell'organo di indirizzo politico;

VISTO il Regolamento di organizzazione della struttura organizzativa e della dirigenza del Consiglio regionale approvato con deliberazione dell'Ufficio di presidenza n. 156 del 11 settembre 2007, come modificato dalle deliberazioni n. 243 del 13 marzo 2008, n. 102 del 30 dicembre 2010, n. 391 del 19 novembre 2018, n. 1 del 11 gennaio 2019 e n. 101 del 20 dicembre 2019;

VISTO il Regolamento di disciplina del funzionamento dell'Ufficio di Presidenza, della formazione e della adozione degli atti amministrativi di competenza del Presidente dell'Assemblea legislativa, dell'Ufficio di presidenza, del Segretario generale e dei dirigenti della Segreteria generale dell'Assemblea legislativa (approvato con deliberazione dell'Ufficio di Presidenza 18 giugno 2018, n. 358 e modificato dalla deliberazione dell'UP n.61/2021), ed in particolare l'articolo 10, comma 1;

DATO ATTO che il presente atto non comporta spese o oneri aggiuntivi per l'Assemblea legislativa;

SI PROPONE DI DELIBERARE

1)-**Di approvare** la Procedura per la notifica di una violazione dei Dati Personali "Data Breach" ai sensi dell'art. 33 del Reg. Ue n. 679/2016 e dell'art. 26 del D.lgs 51/2018 di cui all'**allegato A** che costituisce parte integrante e sostanziale del presente atto;

2)-**Di disporre** che sono sottoposti all'osservanza della Procedura di cui al punto che precede tutti coloro che sono autorizzati al trattamento di dati personali (personale dipen-

dente dell'Assemblea legislativa, personale dipendente e collaboratori dei Gruppi consiliari, i Consiglieri regionali, gli Assessori regionali non Consiglieri);

4)-**Di dare atto** che dal presente atto non derivano spese o oneri aggiuntivi per l'Assemblea legislativa;

5)-**Di dare atto** che il presente atto è soggetto a pubblicazione nel sito istituzionale ai sensi dell'art. 12 del d.lgs. n.33/2013;

6)-Di disporre che il presente atto e l'unito allegato siano pubblicati a cura del responsabile della Sezione Segreteria di direzione, cerimoniale ed educazione alla cittadinanza nel sito istituzionale Sezione amministrazione trasparente nella pagina https://trasparenza.alumbria.it/atti-amministrativi-generali e nella pagina https://trasparenza.alumbria.it/provvedimenti-organi-indirizzo-politico a mezzo collegamento (link) alla prima pubblicazione;

7)-**Di trasmettere** il presente atto e l'unito allegato al RPD interno, al Segretario generale, ai dirigenti, ai componenti della Rete dei referenti privacy, al responsabile della posizione Sezione sistema informatico, ciascuno per il seguito di competenza;

8)-**Di trasmettere** il presente atto e l'unito allegato al personale dipendente dell'Assemblea legislativa, al personale dipendente e ai collaboratori dei Gruppi consiliari, ai Consiglieri regionali, agli Assessori regionali non Consiglieri, al Presidente del Corecom, al Presidente dell'ISUC, al Presidente del CSGP, all'Ufficio di presidenza del CAL, al Difensore civico regionale.

Perugia 21 marzo 2022

L'istruttore
Sabrina Di Cola

Il Segretario generale
Juri Rosi

Palazzo Cesaroni
Piazza Italia, 2
06121 PERUGIA

PARERE DI REGOLARITÀ AMMINISTRATIVA

Ai sensi e per gli effetti degli articoli 10 e 27 del Regolamento approvato con deliberazione dell'Ufficio di presidenza n. 358/2018, come modificato dalla deliberazione dell'UP n.61/2021, si attesta la regolarità amministrativa del presente atto.

Perugia 21 marzo 2022

Il Segretario generale
Juri Rosi

ATTESTAZIONE DI IRRILEVANZA DEL PARERE DI REGOLARITÀ CONTABILE

Ai sensi e per gli effetti dell'articolo 31 bis, comma 2, del Regolamento approvato con deliberazione dell'Assemblea Legislativa n. 284/2018, come modificato con deliberazione n. 114/2021, verificato che il presente atto non comporta spese o riflessi diretti o indiretti sulla situazione economico-finanziaria o sul patrimonio dell'Assemblea Legislativa, si dichiara l'irrilevanza del parere di regolarità contabile.

Perugia 21 marzo 2022

Il Responsabile *ad interim* del Servizio
Risorse e Sistema informativo
Juri Rosi

Regione Umbria
Assemblea legislativa

Palazzo Cesaroni
Piazza Italia, 2 - 06121 PERUGIA
Pec: cons.reg.umbria@arubapec.it
centralino: 075/5761
www.consiglio.regione.umbria.it

ALLEGATO A
della deliberazione dell'Ufficio di presidenza n. 20 del 21 marzo 2022)

Procedura per la notifica di una violazione dei Dati Personali "Data Breach" – art. 33 del Reg. Ue n. 679/2016 e art. 26 del D.lgs 51/2018

Palazzo Cesaroni
Piazza Italia, 2 - 06121 PERUGIA
Pec: cons.reg.umbria@arubapec.it
centralino: 075/5761
www.consiglio.regione.umbria.it

PREMESSA

Il presente documento redatto in collaborazione con il RPD dell'Ente ha l'obiettivo di fornire indicazioni operative per gestire in maniera tempestiva e puntuale una violazione dei dati personali, denominata anche Data Breach così come previsto dall'art. 33 del Reg. UE n. 679/2016 e dall'art. 26 del D.Lgs 51/2018.
Il documento contiene, quindi, sia indicazioni ed informazioni sulle possibili violazioni, sulle varie tipologie delle stesse, le modalità operative da adottare, le figure coinvolte e le varie responsabilità con i relativi tempi di attuazione.

L'art. 33 del Regolamento Europeo 679/2016 (GDPR) e la normativa nazionale in vigore, impongono al Titolare del trattamento di **notificare all'autorità di controllo la violazione di dati personali (data breach) entro** 72 ore dal momento in cui ne viene a conoscenza, per le Pubbliche Amministrazioni come nel caso dell'Assemblea legislativa il tempo è ridotto alle **48 ore**.

L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

1.0 LA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Per **"Violazione di dati"** 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 p.12 del GDPR).

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

Alcuni possibili esempi di violazione:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

Palazzo Cesaroni
Piazza Italia, 2 - 06121 PERUGIA
Pec: cons.reg.umbria@arubapec.it
centralino: 075/5761
www.consiglio.regione.umbria.it

2.0 GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI

Il Titolare del trattamento dove **senza ingiustificato ritardo** e, ove possibile, **entro 48 ore dal momento in cui ne è venuto a conoscenza**, notificare la violazione al Garante per la protezione dei dati personali a meno che sia **improbabile** che la violazione dei dati personali comporti un **rischio** per i diritti e le libertà delle persone fisiche.

Procedura interna da osservare:

Ogni persona autorizzata o designata al trattamento dei dati personali, qualora viene a conoscenza di una eventuale violazione è tenuta ad informare tempestivamente a mezzo email:
-il Segretario generale in quanto delegato dal Titolare del trattamento
-il Referente della Privacy del proprio settore;
-il Responsabile della Sezione sistema informatico Fabio Nardi
-il RPD interno Sabrina Di Cola
specificando quanto segue:

- la natura della violazione dei dati personali compresi;
- ove possibile, le categorie e il numero approssimativo di interessati coinvolti;
- ove possibile, le categorie e il numero approssimativo di registrazioni dei dati personali coinvolti;
- le probabili conseguenze della violazione dei dati personali;
- le eventuali misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Il Segretario generale, in quanto delegato dal Titolare, di concerto con il RPD e con il supporto del consulente esterno, procede alla **valutazione del rischio,** attraverso la metodologia ENISA, e decide se effettuare o meno la comunicazione al Garante ed eventualmente all'interessato/i.

Successivamente il Segretario generale, in quanto delegato dal Titolare del trattamento, eventualmente con il supporto del RPD procede, a prescindere dalla notifica al Garante, ad **annotare e documentare** tutte le violazioni dei dati personali, **nell'apposito Registro**. Tale documentazione consente all'Autorità Garante di effettuare eventuali verifiche sul rispetto della normativa come previsto ai sensi dell'art.33 del Reg. UE n. 679/2016 e art. 26 del D.lgs 51/2018.

Le notifiche al Garante effettuate oltre il termine delle 48 ore **devono essere** accompagnate dai motivi del ritardo e devono essere effettuate telematicamente attraverso autenticazione digitale al presente link: *https://servizi.gpdp.it/databreach.*

Palazzo Cesaroni
Piazza Italia, 2 - 06121 PERUGIA
Pec: cons.reg.umbria@arubapec.it
centralino: 075/5761
www.consiglio.regione.umbria.it

Se la violazione comporta un rischio elevato per i diritti delle persone, il Segretario generale, in quanto delegato dal Titolare, deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.

3.0 NOTIFICA ALL'AUTORITA' GARANTE DELLA PROTEZIONE DEI DATI PERSONALI

Vanno notificate unicamente le violazioni di dati personali che possono avere **effetti avversi significativi** sugli individui, causando danni fisici, materiali o immateriali.

Ciò può includere, ad esempio, la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.