

REGOLAMENTI INTERNI E DI PROCEDURA

DECISIONE DEL CONSIGLIO DI AMMINISTRAZIONE DELL'AGENZIA DELL'UNIONE EUROPEA PER LA CIBERSICUREZZA,

del 21 novembre 2019,

sulle norme interne relative alle limitazioni di determinati diritti degli interessati in relazione al trattamento dei dati personali nell'ambito del funzionamento dell'ENISA

IL CONSIGLIO DI AMMINISTRAZIONE DELL'ENISA

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE ⁽¹⁾, in particolare l'articolo 25, del medesimo,

visto il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersecurity, e alla certificazione della cibersecurity per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 (regolamento sulla cibersecurity ⁽²⁾), e in particolare l'articolo 15, paragrafo 1, del medesimo,

visto il parere del GEPD del 17 ottobre 2019 e gli orientamenti del GEPD sull'articolo 25 del regolamento (UE) 2018/1725 e le norme interne,

considerando quando segue:

- (1) Conformemente all'articolo 25, paragrafo 1, del regolamento (UE) 2018/1725, le limitazioni all'applicazione degli articoli da 14 a 22, 35 e 36, nonché dell'articolo 4 del medesimo regolamento, nella misura in cui le sue disposizioni corrispondano ai diritti e agli obblighi di cui agli articoli da 14 a 22, dovrebbero basarsi sulle norme interne che saranno adottate dall'ENISA, laddove non si basino su atti giuridici adottati in base ai trattati.
- (2) Queste norme interne, comprese le relative disposizioni sulla valutazione della necessità e proporzionalità di una limitazione, non si dovrebbero applicare se un atto giuridico adottato in base ai trattati prevede una limitazione dei diritti degli interessati.
- (3) Laddove eserciti le proprie funzioni rispetto ai diritti degli interessati ai sensi del regolamento (UE) 2018/1725, l'ENISA valuta se sia applicabile una delle deroghe previste in tale regolamento.
- (4) Nell'ambito del proprio operato, l'ENISA può condurre indagini amministrative e procedimenti disciplinari, svolgere attività preliminari riguardanti casi di potenziali irregolarità segnalate all'OLAF, trattare denunce di irregolarità, procedure (formali e informali) di molestie e reclami interni ed esterni, effettuare audit interni, condurre valutazioni sugli incidenti di cibersecurity ai sensi dell'articolo 7, paragrafo 4, del regolamento (UE) 2019/881, condurre indagini svolte dal responsabile della protezione dei dati («RPD»), in linea con l'articolo 45, paragrafo 2, del regolamento (UE) 2018/1725, e indagini interne sulla sicurezza (IT).

L'ENISA tratta diverse categorie di dati personali, tra cui dati controllati (dati «oggettivi», quali dati d'identificazione, recapiti, dati professionali, dettagli amministrativi, dati ricevuti da fonti specifiche, comunicazioni elettroniche e dati sul traffico) e/o dati non controllati (dati «soggettivi» riguardanti il caso, quali motivazione, dati comportamentali, valutazioni, dati su comportamenti e prestazioni e dati relativi o presentati in relazione all'oggetto del procedimento o dell'attività).

- (5) L'ENISA, rappresentata dal suo direttore esecutivo, agisce in qualità di titolare del trattamento, indipendentemente dalle ulteriori deleghe di tale ruolo all'interno dell'ENISA per riflettere le responsabilità operative delle specifiche attività di trattamento dei dati personali.

⁽¹⁾ GUL 295 del 21.11.2018, pag. 39.

⁽²⁾ GUL 151 del 7.6.2019, pag. 15.

- (6) I dati personali sono conservati in modo sicuro in un ambiente elettronico o in formato cartaceo, impedendo l'accesso illecito o il trasferimento dei dati a persone che non hanno necessità di venirne a conoscenza. I dati personali trattati sono conservati solo per il periodo di tempo necessario e opportuno per le finalità del trattamento come specificato nelle comunicazioni sulla protezione dei dati, nelle informative sulla privacy o nei registri dell'ENISA.
- (7) Le norme interne dovrebbero applicarsi a tutti i trattamenti dei dati svolti dall'ENISA quando conduce indagini amministrative, procedimenti disciplinari, attività preliminari riguardanti casi di potenziali irregolarità segnalate all'OLAF, procedure in materia di denunce di irregolarità, procedure (formali e informali) per casi di molestia, quando tratta reclami interni ed esterni, audit interni, valutazioni di incidenti sulla cibersecurity ai sensi dell'articolo 7, paragrafo 4, del regolamento (UE) 2019/881, indagini svolte dal responsabile della protezione dei dati conformemente all'articolo 45, paragrafo 2, del regolamento (UE) 2018/1725, e indagini sulla sicurezza (IT) gestite internamente o mediante intervento esterno (ad esempio CERT-UE).
- (8) Tali norme interne dovrebbero applicarsi alle operazioni di trattamento effettuate prima dell'apertura delle procedure di cui sopra, nel corso di tali procedure e durante il monitoraggio del seguito dei relativi risultati. Dovrebbero essere comprese altresì l'assistenza e la cooperazione fornite dall'ENISA alle autorità nazionali e alle organizzazioni internazionali al di fuori delle proprie indagini amministrative.
- (9) Nei casi in cui si applichino tali regole interne, l'ENISA deve fornire giustificazioni che spieghino il motivo per cui tali limitazioni siano strettamente necessarie e proporzionate in una società democratica e rispettino l'essenza dei diritti e delle libertà fondamentali.
- (10) In questo quadro, l'ENISA è tenuta a rispettare, nella misura più ampia possibile, i diritti fondamentali degli interessati durante i citati procedimenti, in particolare quelli che riguardano il diritto di comunicare informazioni, il diritto di accesso e rettifica, il diritto di cancellazione e limitazione del trattamento, il diritto di comunicazione di una violazione dei dati personali all'interessato o il diritto alla riservatezza delle comunicazioni sancito nel regolamento (UE) n. 2018/1725.
- (11) Tuttavia, l'ENISA può essere costretta a limitare le informazioni all'interessato e altri suoi diritti per proteggere, in particolare, le proprie indagini, le indagini e i procedimenti di altre autorità pubbliche, nonché i diritti di altre persone coinvolte nelle sue indagini o in altre procedure.
- (12) L'ENISA può quindi limitare le informazioni allo scopo di proteggere l'indagine nonché i diritti e le libertà fondamentali degli altri interessati.
- (13) L'ENISA dovrebbe monitorare periodicamente che le condizioni che giustificano la limitazione continuino ad applicarsi e revocare la limitazione non appena cessino di sussistere.
- (14) Il titolare del trattamento dovrebbe informare il responsabile della protezione dei dati al momento del rinvio e durante le revisioni.
- (15) In ragione dell'importanza delle norme interne per la protezione dei diritti degli interessati, la decisione dovrebbe entrare in vigore appena possibile dopo la sua pubblicazione nella *Gazzetta ufficiale dell'Unione europea*,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Oggetto e campo d'applicazione

1. La presente decisione definisce norme relative alle condizioni alle quali l'ENISA, nel quadro delle sue procedure stabilite al paragrafo 2, può limitare l'applicazione dei diritti sanciti negli articoli da 14 a 21, 35 e 36, nonché nell'articolo 4, in base all'articolo 25 del regolamento (UE) n. 2018/1725.
2. Nell'ambito dell'operato dell'ENISA, tale decisione si applica ai trattamenti dei dati personali svolti dall'ENISA ai fini di: condurre indagini amministrative, procedimenti disciplinari, attività preliminari riguardanti casi di potenziali irregolarità segnalate all'OLAF, trattare denunce di irregolarità, procedure (formali e informali) di molestia, reclami interni ed esterni, effettuare audit interni, condurre valutazioni di incidenti di cibersecurity ai sensi dell'articolo 7, paragrafo 4, del regolamento (UE) 2019/881, indagini svolte dal responsabile della protezione dei dati conformemente all'articolo 45, paragrafo 2, del regolamento (UE) 2018/1725, e indagini sulla sicurezza (IT) gestite internamente o mediante intervento esterno (ad esempio CERT-UE).

3. Le categorie di dati interessate sono i dati controllati (dati «oggettivi» quali dati d'identificazione, recapiti, dati professionali, dettagli amministrativi, dati ricevuti da fonti specifiche, comunicazioni elettroniche e dati sul traffico) e/o dati non controllati (dati «soggettivi» riguardanti il caso, quali motivazione, dati comportamentali, valutazioni, dati su comportamenti e prestazioni e dati relativi o presentati in relazione all'oggetto del procedimento o dell'attività).
4. Laddove eserciti le proprie funzioni rispetto ai diritti degli interessati ai sensi del regolamento (UE) 2018/1725, l'ENISA valuta se sia applicabile una delle deroghe previste in tale regolamento.
5. Fatte salve le condizioni stabilite nella presente decisione, le limitazioni si possono applicare ai seguenti diritti: comunicazione di informazioni agli interessati, diritto di accesso, rettifica, cancellazione, limitazione del trattamento, comunicazione di una violazione dei dati personali all'interessato o riservatezza delle comunicazioni.

Articolo 2

Specifiche del titolare del trattamento e garanzie

1. Le garanzie predisposte per prevenire violazioni, sottrazioni di dati o divulgazioni non autorizzate sono le seguenti:
 - a) i documenti cartacei sono tenuti in armadi sicuri e accessibili soltanto al personale autorizzato;
 - b) tutti i dati elettronici sono memorizzati in un'applicazione informatica sicura conformemente agli standard di sicurezza dell'ENISA e in specifiche cartelle elettroniche accessibili unicamente al personale autorizzato. Sono disposti appropriati livelli di accesso su base individuale;
 - c) la banca dati è protetta da password nell'ambito di un sistema di accesso SSO (Single Sign On) ed è collegata automaticamente all'ID dell'utente e alla password. La sostituzione degli utenti è rigorosamente vietata. I registri elettronici sono conservati in maniera sicura per tutelare la riservatezza e la segretezza dei dati contenuti;
 - d) tutte le persone che hanno accesso ai dati hanno l'obbligo della riservatezza.
2. Il titolare del trattamento è l'ENISA, rappresentata dal suo direttore esecutivo, il quale può delegare la funzione di titolare. Gli interessati sono informati riguardo ai titolari del trattamento delegati attraverso comunicazioni sulla protezione dei dati o registri pubblicati nel sito Internet e/o sull'Intranet dell'ENISA.
3. Il periodo di conservazione dei dati personali di cui all'articolo 1, paragrafo 3, non deve essere più lungo di quanto necessario e opportuno per le finalità del trattamento. In ogni caso, non deve superare il periodo di conservazione specificato nelle comunicazioni sulla protezione dei dati, nelle informative sulla privacy o nei registri di cui all'articolo 5, paragrafo 1.
4. Qualora l'ENISA consideri di applicare una limitazione, si valuta il rischio per i diritti e le libertà dell'interessato, in particolare rispetto al rischio per i diritti e le libertà degli altri interessati e al rischio di annullare gli effetti delle indagini o delle procedure dell'ENISA, ad esempio distruggendo gli elementi di prova. I rischi per i diritti e le libertà dell'interessato riguardano principalmente, ma non esclusivamente, i rischi legati alla reputazione e i rischi per il diritto di difesa e il diritto di essere ascoltato.

Articolo 3

Limitazioni

1. Eventuali limitazioni sono applicate dall'ENISA esclusivamente per salvaguardare:
 - a) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e relativa prevenzione;
 - b) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare gli obiettivi della politica estera e di sicurezza comune dell'Unione o un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale;
 - c) la sicurezza interna delle istituzioni e degli organismi dell'Unione, comprese le relative reti di comunicazione elettronica;

- d) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;
- e) una funzione di controllo, ispezione o regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere a) e b);
- f) la tutela dell'interessato o dei diritti e delle libertà altrui.

2. La valutazione degli incidenti di cibersicurezza svolta dall'ENISA ai sensi dell'articolo 7, paragrafo 4, del regolamento (UE) 2019/881 (regolamento sulla cibersicurezza) è prevista nel paragrafo 1, lettera b), del presente articolo.

3. Come applicazione specifica delle finalità descritte nel precedente paragrafo 1, l'ENISA può applicare limitazioni riguardanti i dati personali scambiati con i servizi della Commissione o altre istituzioni, organi e organismi dell'Unione, autorità competenti degli Stati membri o paesi terzi o organizzazioni internazionali nei seguenti casi:

- a) quando l'esercizio di tali diritti e obblighi potrebbe essere limitato dai servizi della Commissione o da altre istituzioni, organi e organismi dell'Unione in virtù di altri motivi previsti dall'articolo 25 del regolamento (UE) 2018/1725, conformemente al capo IX di detto regolamento, oppure sulla base degli atti costitutivi di altre istituzioni, organi e organismi dell'Unione;
- b) quando l'esercizio di tali diritti e obblighi potrebbe essere limitato dalle autorità competenti degli Stati membri sulla base dei motivi di cui all'articolo 23 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ^(*) o a norma delle disposizioni nazionali di recepimento dell'articolo 13, paragrafo 3, dell'articolo 15, paragrafo 3, o dell'articolo 16, paragrafo 3, della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio ^(*);
- c) quando l'esercizio di tali diritti e obblighi potrebbe pregiudicare la cooperazione dell'ENISA con paesi terzi o organizzazioni internazionali nello svolgimento dei suoi compiti.

Prima di applicare limitazioni nei casi di cui al primo comma, lettere a) e b), l'ENISA consulta i servizi della Commissione, le istituzioni, gli organi e gli organismi dell'Unione pertinenti o le autorità competenti degli Stati membri, a meno che all'ENISA non risulti evidente che l'applicazione di una limitazione è prevista in virtù di uno dei motivi di cui alle summenzionate lettere.

4. Le eventuali limitazioni sono necessarie e proporzionate tenuto conto dei rischi per i diritti e le libertà degli interessati e rispettano l'essenza dei diritti e delle libertà fondamentali in una società democratica.

5. Se si considera l'applicazione di limitazioni, si effettua una verifica della necessità e della proporzionalità sulla base delle presenti norme. Tale procedura è documentata mediante una nota di valutazione interna ed è effettuata caso per caso.

6. Le limitazioni sono revocate non appena le condizioni che le giustificano cessino di sussistere. In particolare, laddove si ritenga che l'esercizio del diritto ristretto non annullerebbe più l'effetto della limitazione imposta o lederebbe i diritti e le libertà degli altri interessati.

Articolo 4

Revisione da parte del responsabile della protezione dei dati

1. L'ENISA informa senza indebito ritardo il proprio responsabile della protezione dei dati ogniqualvolta il titolare del trattamento limiti l'applicazione dei diritti degli interessati o estenda la limitazione, a norma della presente decisione. Il titolare del trattamento fornisce al responsabile della protezione dei dati l'accesso al registro che contiene la valutazione della necessità e della proporzionalità della limitazione e documenta nel registro la data in cui lo ha informato. L'ENISA coinvolge il responsabile della protezione dei dati in tutte le procedure pertinenti documentando tale coinvolgimento.

2. Il responsabile della protezione dei dati può chiedere per iscritto al titolare del trattamento di riesaminare l'applicazione delle limitazioni. Il titolare del trattamento informa per iscritto il proprio responsabile della protezione dei dati circa l'esito del riesame richiesto.

^(*) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

^(*) 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 (GU L 119 del 4.5.2016, pag. 89).

3. Il titolare del trattamento informa il responsabile della protezione dei dati quando la limitazione cessa di sussistere.

Articolo 5

Comunicazione di informazioni agli interessati

1. In casi debitamente giustificati e alle condizioni stabilite nella presente decisione, il diritto all'informazione può essere limitato dal titolare del trattamento nell'ambito dei seguenti trattamenti:

- a) svolgimento di indagini amministrative e procedimenti disciplinari;
- b) attività preliminari riguardanti casi di potenziali irregolarità segnalate all'OLAF;
- c) procedure in materia di denunce di irregolarità;
- d) procedure (formali e informali) per casi di molestia;
- e) trattamento di reclami interni ed esterni;
- f) audit interni;
- g) indagini svolte dal responsabile della protezione dei dati, in linea con l'articolo 45, paragrafo 2, del regolamento (UE) 2018/1725;
- h) indagini sulla sicurezza (IT) gestite internamente o mediante intervento esterno (ad esempio CERT-UE);
- i) valutazioni degli incidenti di cibersicurezza svolte dall'ENISA ai sensi dell'articolo 7, paragrafo 4, del regolamento (UE) 2019/881, in linea con l'articolo 3, paragrafo 2, della presente decisione.

Nelle comunicazioni sulla protezione dei dati, nelle informative sulla privacy e nei registri, ai sensi dell'articolo 31 del regolamento (UE) 2018/1725, pubblicati sul proprio sito Internet e/o sull'Intranet, che informano gli interessati sui loro diritti nel quadro di una determinata procedura, l'ENISA include informazioni riguardanti le potenziali limitazioni di questi diritti. Tali informazioni riguardano i diritti che possono essere limitati, le ragioni e la durata potenziale della limitazione.

2. Fatte salve le disposizioni di cui al paragrafo 3 del presente articolo, se proporzionato, l'ENISA informa inoltre, senza indebito ritardo e in forma scritta, singolarmente tutti gli interessati considerati persone interessate nella specifica operazione di trattamento, dei loro diritti riguardanti le limitazioni attuali o future.

3. Qualora limiti, in tutto o in parte, la comunicazione di informazioni agli interessati di cui al paragrafo 2 del presente articolo, l'ENISA registra le ragioni della limitazione, il motivo giuridico conformemente all'articolo 3 della presente decisione, inclusa la valutazione della necessità e della proporzionalità della limitazione.

La registrazione e, ove applicabile, i documenti contenenti gli elementi di fatto e di diritto che ne costituiscono la base sono conservati in un registro. Su richiesta, essi sono messi a disposizione del Garante europeo della protezione dei dati.

4. La limitazione di cui al paragrafo 3 del presente articolo continua ad applicarsi finché permangono i motivi che la giustificano.

Qualora i motivi della limitazione non siano più applicabili, l'ENISA fornisce all'interessato le informazioni sulle ragioni principali alla base dell'applicazione di una limitazione. Nel contempo l'ENISA informa l'interessato del diritto di presentare in qualsiasi momento reclamo al Garante europeo della protezione dei dati o un ricorso giurisdizionale dinanzi alla Corte di giustizia dell'Unione europea.

L'ENISA riesamina l'applicazione della limitazione ogni sei mesi dalla sua adozione e all'atto della chiusura dell'inchiesta, della procedura o dell'indagine pertinente. Successivamente il titolare del trattamento valuta la necessità di mantenere eventuali limitazioni ogni sei mesi.

Articolo 6

Diritto di accesso dell'interessato

1. In casi debitamente giustificati e alle condizioni stabilite nella presente decisione, il diritto di accesso può essere limitato dal titolare del trattamento, laddove necessario e proporzionato, nel contesto dei seguenti trattamenti:

- a) svolgimento di indagini amministrative e procedimenti disciplinari;
- b) attività preliminari riguardanti casi di potenziali irregolarità segnalate all'OLAF;
- c) procedure in materia di denunce di irregolarità;

- d) procedure (formali e informali) per casi di molestia;
- e) trattamento di reclami interni ed esterni;
- f) audit interni;
- g) indagini svolte dal responsabile della protezione dei dati, in linea con l'articolo 45, paragrafo 2, del regolamento (UE) 2018/1725;
- h) indagini sulla sicurezza (IT) gestite internamente o mediante intervento esterno (ad esempio CERT-UE);
- i) valutazioni degli incidenti di cibersicurezza svolte dall'ENISA ai sensi dell'articolo 7, paragrafo 4, del regolamento (UE) 2019/881, in linea con l'articolo 3, paragrafo 2, della presente decisione.

Qualora, a norma dell'articolo 17 del regolamento (UE) 2018/1725, gli interessati chiedano l'accesso ai propri dati personali trattati nell'ambito di uno o più casi specifici o di particolari trattamenti, l'ENISA limita la propria valutazione della richiesta esclusivamente a tali dati personali.

2. Allorché limita, integralmente o in parte, il diritto di accesso di cui all'articolo 17 del regolamento (UE) 2018/1725, l'ENISA procede nel modo seguente:

- a) informa l'interessato, nella propria risposta alla richiesta, in merito alla limitazione applicata e ai principali motivi della stessa, come pure alla possibilità di presentare reclamo al Garante europeo della protezione dei dati o di proporre un ricorso giurisdizionale dinanzi alla Corte di giustizia dell'Unione europea;
- b) registra in una nota di valutazione interna i motivi della limitazione, compresa una valutazione della necessità e della proporzionalità della limitazione e della sua durata.

La comunicazione di informazioni di cui alla lettera a) può essere rinviata, omessa o negata se annullasse l'effetto della limitazione in conformità dell'articolo 25, paragrafo 8, del regolamento (UE) 2018/1725.

L'ENISA riesamina l'applicazione della limitazione ogni sei mesi dalla sua adozione e all'atto della chiusura dell'indagine pertinente. Successivamente il titolare del trattamento valuta la necessità di mantenere eventuali limitazioni ogni sei mesi.

3. L'annotazione e, se del caso, i documenti contenenti gli elementi di fatto e di diritto che ne costituiscono la base sono conservati in un registro. Su richiesta, essi sono messi a disposizione del Garante europeo della protezione dei dati.

Articolo 7

Diritto di rettifica, cancellazione e limitazione del trattamento

1. In casi debitamente giustificati e alle condizioni stabilite nella presente decisione, il diritto di rettifica, cancellazione e limitazione può essere limitato dal titolare del trattamento, laddove necessario e opportuno, nel contesto dei seguenti trattamenti:

- a) svolgimento di indagini amministrative e procedimenti disciplinari;
- b) attività preliminari riguardanti casi di potenziali irregolarità segnalate all'OLAF;
- c) procedure in materia di denunce di irregolarità;
- d) procedure (formali e informali) per casi di molestia;
- e) trattamento di reclami interni ed esterni;
- f) audit interni;
- g) indagini svolte dal responsabile della protezione dei dati, in linea con l'articolo 45, paragrafo 2, del regolamento (UE) 2018/1725;
- h) indagini sulla sicurezza (IT) gestite internamente o mediante intervento esterno (ad esempio CERT-UE);
- i) valutazioni degli incidenti di cibersicurezza svolte dall'ENISA ai sensi dell'articolo 7, paragrafo 4, del regolamento (UE) 2019/881, in linea con l'articolo 3, paragrafo 2, della presente decisione.

2. Qualora limiti, integralmente o in parte, l'applicazione del diritto di rettifica, cancellazione o limitazione di trattamento di cui all'articolo 18, all'articolo 19, paragrafo 1, e all'articolo 20, paragrafo 1, del regolamento (UE) 2018/1725, l'ENISA adotta le misure di cui all'articolo 6, paragrafo 2, della presente decisione e in conformità dell'articolo 6, paragrafo 3, della stessa.

*Articolo 8***Comunicazione di una violazione dei dati personali all'interessato e riservatezza delle comunicazioni elettroniche**

1. In casi debitamente giustificati e alle condizioni stabilite nella presente decisione, la comunicazione di una violazione dei dati personali può essere limitata dal titolare del trattamento, laddove necessario e appropriato, nel contesto dei seguenti trattamenti:

- a) svolgimento di indagini amministrative e procedimenti disciplinari;
- b) attività preliminari riguardanti casi di potenziali irregolarità segnalate all'OLAF;
- c) procedure in materia di denunce di irregolarità;
- d) trattamento di reclami interni ed esterni;
- e) audit interni;
- f) indagini svolte dal responsabile della protezione dei dati, in linea con l'articolo 45, paragrafo 2, del regolamento (UE) 2018/1725;
- g) indagini sulla sicurezza (IT) gestite internamente o mediante intervento esterno (ad esempio CERT-UE);
- h) valutazioni degli incidenti di cibersicurezza svolte dall'ENISA ai sensi dell'articolo 7, paragrafo 4, del regolamento (UE) 2019/881, in linea con l'articolo 3, paragrafo 2, della presente decisione.

2. In casi debitamente giustificati e alle condizioni stabilite nella presente decisione, la riservatezza delle comunicazioni elettroniche può essere limitata dal titolare del trattamento, laddove necessario e appropriato, nel contesto dei seguenti trattamenti:

- a) svolgimento di indagini amministrative e procedimenti disciplinari;
- b) attività preliminari riguardanti casi di potenziali irregolarità segnalate all'OLAF;
- c) procedure in materia di denunce di irregolarità;
- d) procedure formali di casi di molestia;
- e) trattamento di reclami interni ed esterni;
- f) indagini sulla sicurezza (IT) gestite internamente o mediante intervento esterno (ad esempio CERT-UE);
- g) valutazioni degli incidenti di cibersicurezza svolte dall'ENISA ai sensi dell'articolo 7, paragrafo 4, del regolamento (UE) 2019/881, in linea con l'articolo 3, paragrafo 2, della presente decisione.

3. Laddove limiti la comunicazione delle violazioni dei dati personali agli interessati o la riservatezza delle comunicazioni elettroniche di cui agli articoli 35 e 36 del regolamento (UE) 2018/1725, l'ENISA applica le disposizioni di cui all'articolo 5, paragrafo 3, della presente decisione. Si applica l'articolo 5, paragrafo 4, della presente decisione.

*Articolo 9***Entrata in vigore**

La presente decisione entra in vigore il giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Redatto ad Atene, il 21 novembre 2019

per ENISA

Jean Baptiste DEMAISON

Presidente del consiglio di amministrazione
