REGIONE EMILIA-ROMAGNA

Atti amministrativi

AGENZIA LAVORO

Atto del Dirigente DETERMINAZIONE

Num. 1141 del 09/11/2018 BOLOGNA

Proposta:	DLV/2018/1161 del 06/11/2018
Struttura proponente:	AGENZIA REGIONALE PER IL LAVORO
Oggetto:	RECEPIMENTO DA PARTE DELL'AGENZIA REGIONALE PER IL LAVORO DELLA DELIBERAZIONE DI GIUNTA REGIONALE N. 1123/2018: RIPARTIZIONE DELLE COMPETENZE IN TEMA DI PRIVACY E LINEE GUIDA PRIVACY DELL'AGENZIA REGIONALE PER IL LAVORO
Autorità emanante:	IL DIRETTORE - AGENZIA REGIONALE PER IL LAVORO
Firmatario:	PAOLA CICOGNANI in qualità di Direttore
Responsabile del procedimento:	Paola Cicognani

Firmato digitalmente

IL DIRETTORE

Premesso che:

- il “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)” (di seguito Regolamento), a norma dell’articolo 99 “Entrata in vigore e applicazione”, comma 1 dello stesso Regolamento è entrato in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta dell’Unione europea;
- il Decreto Legislativo n.101/2018, di adeguamento dell’ordinamento italiano al regolamento europeo in materia di trattamento dati personali, è stato pubblicato sulla Gazzetta Ufficiale del 4 settembre 2018, ed è entrato in vigore il 19 settembre 2018, adeguando all’ordinamento europeo il D.lgs. 196/2003 - Codice in materia di protezione dei dati personali;
- l’articolo 99 comma 2 del Regolamento specifica che si applica a decorrere dal 25 maggio 2018 ed è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Dato atto che il Regolamento detta una complessa disciplina di carattere generale in materia di dati personali, prevedendo molteplici obblighi ed adempimenti a carico dei soggetti che trattano dati personali, comprese le pubbliche amministrazioni.

Considerato che:

- l’applicazione del nuovo Regolamento comporta modifiche ricadenti anche sull’assetto organizzativo e sulla ripartizione dei compiti e delle responsabilità in materia di protezione dei dati personali;
- per adeguarsi alle nuove disposizioni contenute nel Regolamento occorre ridefinire l’assetto complessivo del Sistema Regionale, specificando le nuove ripartizioni delle competenze e delle responsabilità in materia di protezione dei dati personali;

Richiamate le deliberazioni della Giunta regionale dell’Emilia-Romagna:

- n. 2416/2008, Appendice 5, e n. 2169/2017, Allegato A e B, che disciplinano l’attuale assetto organizzativo della Giunta in materia di privacy e sicurezza informatica e definiscono un nuovo assetto di compiti e responsabilità e comportano il superamento delle disposizioni contenute negli atti precedenti;
- n. 243/2018 “Approvazione schema di intesa tra Regione Emilia-Romagna e Agenzia regionale per il lavoro per assicurare le funzioni del DPO” sottoscritta in data 22 febbraio 2018 con protocollo LV/2018/0007768 del 2 marzo 2018

Richiamate le proprie determinazioni:

- n. 1306/2017 “Delega di compiti e funzioni in materia di trattamento dei dati personali ai dirigenti responsabili di servizio e ai dirigenti responsabili di ambito territoriale della Agenzia Regionale per il Lavoro”;
- n. 214/2018 “Incarico al DPO della regione Emilia-Romagna delle funzioni in materia di privacy di cui al regolamento (UE) 2016/679”, definite dall’intesa tra regione Emilia-Romagna e Agenzia Regionale per il lavoro del 22/02/2018 che definisce le funzioni del DPO dell’ARL

Richiamato l’accordo, stipulato ai sensi dell’art. 15 della L. 241/1990 e ss.mm. tra la Regione Emilia-Romagna e l’Agenzia Regionale per il Lavoro, per lo svolgimento di attività di supporto all’Agenzia, nello specifico l’art. 1 lettera A) relativo alla fornitura dei servizi ICT di supporto, in accordo col nuovo modello di governance, definito con la deliberazione della Giunta Regionale 1718/2016;

Richiamata l’intesa, tra la Regione Emilia-Romagna e l’Agenzia Regionale per il lavoro intesa per assicurare le funzioni del data protection officer (DPO) protocollo LV/2018/0007768 del 2/3/2018.

Dato atto, in particolare, che la delibera sopracitata n.2169/2017 che designa il Responsabile della Protezione dei Dati (DPO) gli affida il mandato di dare indicazioni sulle modifiche da apportare all’Appendice 5 della delibera 2416/2008;

Visto che l'Allegato A, parte integrante e sostanziale della presente determinazione, formulato sulla base delle indicazioni fornite dal DPO specifica, tra le altre cose, i compiti del DPO e dell’RPCT relativamente alla materia;

Visto che l'Allegato B, parte integrante e sostanziale della presente determinazione formulato sulla base delle indicazioni fornite dal DPO risponde anche all’obbligo di “formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo” come specificato dall’art. 39 del Regolamento (UE) 2016/679 e specificato all’art. 1 lettera k della determina dell’ARL n. 214/2018 sopra richiamata;

Visto il D.lgs. 14 marzo 2013, n. 33 “Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni” e ss.mm.ii.;

Viste inoltre le proprie determinazioni:

- n. 1306/2017 “Delega di compiti e funzioni in materia di trattamento dei dati personali ai dirigenti responsabili di servizio e ai dirigenti responsabili di ambito territoriale della agenzia regionale per il lavoro”
- n. 162/2016 “Individuazione degli incaricati del trattamento dei dati personali nell’ambito dell’Agenzia regionale per il lavoro – sedi territoriali, ai sensi del D.lgs. 196/2003 (2017)”
- n. 100/2018 “Approvazione del piano triennale di prevenzione della corruzione - 2018/2020 e nomina del responsabile della prevenzione della corruzione e della trasparenza dell'agenzia regionale per il lavoro”

- n. 129/2018 “Approvazione della mappatura aree a rischio corruzione processi e misure anno 2018 ad integrazione della determinazione n. 100 del 31/1/2018 approvazione del piano triennale per la prevenzione della corruzione anni 2018-2020 e nomina del responsabile della prevenzione della corruzione e della trasparenza dell'agenzia regionale per il lavoro";

Acquisito con nostro protocollo LV/2018/0043208 del 13/11/2018 il parere del DPO dell’ARL in merito al presente atto, all’Allegato A) e all’Allegato B). e recepite nel presente atto tutte le proposte di modifica giunte dal DPO;

Attestata, ai sensi della delibera di Giunta 2416/2008 e s.m.i., la regolarità del presente atto;

D E T E R M I N A

1) di approvare l’Allegato A) quale parte integrante e sostanziale del presente atto;
2) di approvare l’Allegato B) quale parte integrante e sostanziale del presente atto;
3) di abrogare la determina n. 1306 del 13/12/2017, le cui disposizioni sono integralmente sostituite da quanto approvato con il presente atto;
4) di recepire l’abrogazione dell'Appendice 5 della deliberazione della Giunta regionale n. 2416/2008 e ss.mm.ii., le cui disposizioni sono integralmente sostituite da quanto approvato con la deliberazione della Giunta regionale n.1123/2018
5) di recepire l’abrogazione dell’Allegato A e dell’Allegato B della deliberazione della Giunta regionale n. 2169/2017;
6) di dare atto, infine, che per quanto previsto in materia di pubblicità, trasparenza e diffusione di informazioni, si provvederà ai sensi delle disposizioni normative e amministrative richiamate in parte narrativa.

Paola Cicognani

AGENZIA REGIONALE PER IL LAVORO EMILIA-ROMAGNA

ALLEGATO A

DEFINIZIONE DI COMPETENZE E RESPONSABILITA' IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Sommario

1. Indirizzi generali

Il 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 (di seguito anche solo "Regolamento"), detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi ed adempimenti a carico dei soggetti che trattano dati personali, ivi comprese le pubbliche amministrazioni.

Le disposizioni del D.lgs. 196/2003 "Codice in materia di protezione dei dati personali" così come modificato dal D.Lgs 101/2018 e altre modifiche e integrazioni, nonché i Provvedimenti di carattere generale emanati dal Garante per la protezione dei dati personali (di seguito anche solo "Garante"), continuano a trovare applicazione nella misura in cui non siano in contrasto con la normativa succitata.

Per dare attuazione ai suddetti obblighi ed adempimenti, occorre rivedere l'assetto delle responsabilità all'interno dell'Agenzia Regionale per il lavoro (di seguito ARL).

Il regolamento europeo individua diversi attori che intervengono nei trattamenti di dati personali effettuati dalle organizzazioni, ciascuno con funzioni e compiti differenti:

a) **il Titolare del trattamento**: la 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;

b) **il Responsabile del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

c) **il Responsabile della protezione dei dati** (di seguito anche Data Protection Officer o DPO): figura prevista dagli artt. 37 e ss. del regolamento, che ne disciplinano compiti, funzioni e responsabilità;

d) **persone autorizzate al trattamento dei dati personali** sotto l'autorità diretta del titolare o del responsabile: figura che si desume implicitamente dalla definizione di "terzo" di cui al n. 10 del comma 1 art. 4 del Regolamento e dall'articolo 29 del Regolamento, che pone l'obbligo di dare istruzioni a chi abbia accesso a dati personali e agisca sotto la titolarità del titolare o del responsabile.

Con il presente documento l'ARL:

- definisce il proprio ambito di titolarità;
- definisce le funzioni e i compiti del direttore e dei dirigenti dell'ARL, ciascuno per la propria parte di competenza, per l'attuazione degli adempimenti previsti dalla normativa;
- indica i compiti assegnati al DPO designato;
- recepisce i compiti della struttura competente in materia di gestione della sicurezza delle informazioni di cui si avvale come da DGR n.1123 del 16.07.2018;
- recepisce funzioni e compiti del Gruppo dei referenti privacy di cui fa parte come da DGR n.1123 del 16.07.2018;
- definisce i criteri generali da rispettare nell'individuazione dei soggetti autorizzati a compiere le operazioni di trattamento delineando il complessivo ambito delle responsabilità.

2. Il titolare – Funzioni

Titolare dei trattamenti di dati personali, ai sensi dell'art. 4 n. 7 e art. 24 del Regolamento europeo, è l'Agenzia Regionale per il lavoro cui spetta l'adozione di misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento. Spetta pertanto in particolare al direttore dell'ARL:

a) adottare, nelle forme previste dal proprio ordinamento, gli interventi normativi necessari;

b) designare il Responsabile della protezione dei dati, specificando i compiti assegnati;

c) attribuire funzioni e compiti degli adempimenti previsti dalla normativa in materia di trattamento di dati personali;

d) allocare adeguate risorse per la formazione dei dipendenti e collaboratori in materia di protezione dei dati e sicurezza informatica.

e) verificare la legittimità dei trattamenti di dati personali effettuati dall'ARL;

f) disporre, in conseguenza alla verifica di cui alla lett. a) le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;

g) adottare soluzioni di privacy by design e by default;

h) tenere costantemente aggiornato il registro delle attività di trattamento dell'ARL;

i) predisporre le informative relative al trattamento dei dati personali nel rispetto dell'art. 13 del Regolamento;

j) individuare i soggetti autorizzati a compiere operazioni di trattamento (di seguito anche "incaricati" o "autorizzati") fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite; tale individuazione deve essere effettuata in aderenza alle indicazioni contenute nel presente atto e, in particolare, facendo espresso richiamo alle policy regionali in materia di sicurezza informatica e protezione dei dati personali;

k) predisporre ogni adempimento organizzativo necessario per garantire agli interessati l'esercizio dei diritti previsti dalla normativa;

l) provvedere, anche tramite gli incaricati, a dare riscontro alle istanze degli interessati inerenti l'esercizio dei diritti previsti dalla normativa;

m) disporre l'adozione dei provvedimenti imposti dal Garante;

n) collaborare con il DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;

o) adottare, se necessario, specifici Disciplinari tecnici di settore, anche congiuntamente con altri Soggetti delegati all'attuazione, per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali relativi all'ARL;

p) individuare, negli atti di costituzione di gruppi di lavoro comportanti il trattamento di dati personali, i soggetti che effettuano tali trattamenti quali incaricati, specificando, nello stesso atto di costituzione, anche le relative istruzioni;

q) garantire al Responsabile del Servizio competente in materia di sistemi informativi della Giunta regionale e al DPO i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;

r) designare gli amministratori di sistema in aderenza alle norme vigenti in materia;

s) effettuare preventiva valutazione d'impatto ai sensi dell'art. 35 del Regolamento nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la

natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

t) consulta il Garante per la protezione dei dati personali qualora la valutazione d'impatto di cui al punto precedente indichi che il trattamento presenterebbe un rischio elevato nonostante le misure adottate;

u) recepire la policy regionale in materia di sviluppo delle applicazioni da richiamare obbligatoriamente nei contratti di sviluppo di software e piattaforme, disponendo che il mancato rispetto dei requisiti ivi previsti equivale a grave inadempimento, con facoltà per l'ARL di risoluzione del contratto;

v) designare i Responsabili del trattamento con le modalità indicate nel paragrafo 4 del presente atto;

w) recepire eventualmente i disciplinari tecnici trasversali della Giunta della Regione Emilia-Romagna che si rendessero necessari;

x) comunicare degli atti di notifica e di consultazione preventiva all'autorità di controllo;

y) la notifica e la comunicazione delle violazioni dei dati personali all'autorità di controllo ai sensi degli artt. 33 e 34 del Regolamento.

Nell'attuazione dei compiti sopraindicati il direttore dell'ARL può acquisire il parere del DPO nei casi e con le modalità specificate nel successivo paragrafo 7.

Fermo restando che la responsabilità delle attività sopraindicate rimane in ogni caso in capo al direttore dell'ARL, sono delegati i compiti di cui alle lettere e), f), g), h), i), j), n), p), q), r), u), v) ai dirigenti dell'ARL.

3. I responsabili del trattamento

Sono designati responsabili del trattamento di dati personali i soggetti esterni all'amministrazione che siano tenuti, a seguito di convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina, ad effettuare trattamenti di dati personali per conto del titolare.

Pertanto, qualora occorra affidare un incarico comportante anche trattamenti di dati personali, la scelta del soggetto deve essere effettuata valutando anche l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali del soggetto cui affidare l'incarico, affinché lo stesso soggetto sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.

Attesa la natura negoziale delle designazioni dei responsabili del trattamento, questa deve essere effettuata all'interno di contratti o convenzioni e, in ogni caso, in costanza di formazione del rapporto contrattuale, in aderenza ai fac-simili messi a disposizione.

4. I soggetti autorizzati al compimento delle operazioni di trattamento (incaricati/autorizzati)

Sono autorizzati alle operazioni di trattamento dei dati il direttore dell'ARL ed i dirigenti delegati ai sensi della presente disciplina. Essi conformano i loro trattamenti alle policy regionali in materia di protezione dei dati personali e alle seguenti istruzioni:

- sono trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento;

- sono verificati legittimità e correttezza dei trattamenti, avendo particolare attenzione ai rischi che gli stessi presentano e alla natura dei dati personali da proteggere.

Inoltre, devono essere autorizzati tutti i soggetti (di seguito “incaricati” o “ autorizzati”), dipendenti e collaboratori a qualsiasi titolo, che effettuino operazioni di trattamento di dati personali sotto la diretta autorità del Titolare. Gli incaricati devono essere formalmente autorizzati dal Titolare o dai dirigenti delegati.

Gli incaricati sono quindi designati:

a) tramite assegnazione funzionale della persona fisica alla unità organizzativa di minori dimensioni, qualora la persona fisica effettui tutti i trattamenti individuati puntualmente per tale unità.
b) tramite individuazione nominativa (nome e cognome) delle persone fisiche. In questo caso occorre specificare, per ciascun nominativo, i trattamenti che lo stesso è autorizzato ad effettuare;

L’autorizzazione scritta deve inoltre contenere le istruzioni impartite agli incaricati del trattamento di dati personali. Tali istruzioni, oltre a riguardare eventuali aspetti di dettaglio da diversificare in relazione alle specificità dei singoli trattamenti, devono quanto meno contenere un espresso richiamo alle policy regionali in materia di sicurezza informatica e protezione dei dati personali.

5. Il Responsabile della Protezione dei dati – DPO: funzioni e compiti

Il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 prevede l’obbligo per gli Enti pubblici di designare il Responsabile della protezione dei dati (Data Protection Officer, di seguito DPO). L’ARL tramite l’intesa sottoscritta con la Regione Emilia-Romagna ha deciso di avvalersi del supporto del DPO regionale (prot. LV/2018/0007768 del 02.03.2018) con una attribuzione formale di incarico triennale (prot. DLV/2018/231).

Specificatamente, sono di seguito indicati i compiti del DPO in aderenza agli art. 37 e seguenti del suddetto regolamento, in coerenza con l’organizzazione dell’ARL:

a) informa e fornisce consulenza all’ARL in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati personali, con il supporto del Gruppo dei referenti privacy di cui al successivo paragrafo 9;

b) sorveglia l'osservanza della normativa in materia di protezione dei dati personali nonché delle politiche dell’ARL in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) coopera con il Garante per la protezione dei dati personali;

d) funge da punto di contatto per l'Autorità Garante per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento ed effettua, se del caso, consultazioni relativamente a qualunque altra questione;

e) partecipa allo svolgimento delle verifiche di sicurezza svolte dal Responsabile del Servizio ICT regionale o ne richiede di specifiche;

f) promuove la formazione di tutto il personale dell’ARL in materia di protezione dei dati personali e sicurezza informatica, anche attraverso un piano di comunicazione e divulgazione all’interno dell’ARL;

g) partecipa alla gestione degli incidenti di sicurezza nelle modalità previste da specifica policy dell’ARL;

h) formula gli indirizzi per la realizzazione del Registro delle attività di trattamento di cui all’art. 30 del Regolamento;

i) fornisce i pareri obbligatori e facoltativi richiesti dalle strutture secondo quanto specificato al successivo paragrafo 7.

6. Pareri del DPO

Il DPO fornisce il proprio parere in ordine alla legittimità e alla correttezza dei trattamenti di dati personali sulle istanze che le strutture dell'ARL presentano nei casi di seguito indicati.

6.1 Pareri obbligatori

Devono essere obbligatoriamente richiesti pareri in ordine a:

a) individuazione delle misure che abbiano un significativo impatto sulla protezione dei dati personali che l'ARL intende adottare ai fini della tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell'ARL, anche a seguito di incidenti di sicurezza o analisi dei rischi;

b) adozione di policy e disciplinari in materia di protezione dei dati personali e sicurezza delle informazioni, redazione e aggiornamento dei disciplinari tecnici trasversali e di settore con impatto sulla sicurezza delle informazioni;

c) individuazione di misure poste a mitigazione del rischio delle criticità emerse dall'analisi dei rischi, che abbiano un significativo impatto sulla protezione dei dati personali;

d) valutazione del rischio per i diritti e le libertà delle persone fisiche nei casi di data breach.

6.2 Pareri facoltativi

Possono essere inoltre richiesti, se ritenuti utili, pareri in ordine a:

a) progettazione di nuove applicazioni o modifica sostanziale di quelle esistenti, in aderenza al principio della privacy by design e by default;

b) valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35 del Regolamento;

c) valutazione dell'eventuale pregiudizio che l'accesso civico potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alle tutele dei loro dati personali ai sensi del comma 2 dell'art. 5-bis e, in via generale, del Regolamento UE n. 679/2016;

d) opposizione formulata dai controinteressati nella misura in cui questa sia riferibile ad elementi afferenti alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli opponenti, con riscontro del DPO entro tre giorni.

Le richieste di parere devono essere inviate all'indirizzo di posta elettronica dpo@regione.emilia-romagna.it o nelle modalità che saranno stabilite dal DPO stesso.

Possono presentare le richieste di parere il direttore o i dirigenti dell'ARL.

I pareri sono espressi nel rispetto delle seguenti codifiche:

- NC: acronimo di "non conformità", nei casi in cui siano rilevati elementi di non conformità alla normativa e alle policy regionali in materia di protezione dei dati personali;
- OS: acronimo di "osservazione", nei casi in cui vi siano elementi di miglioramento che garantiscono una maggiore aderenza alla normativa e alle policy regionali in materia di protezione dei dati personali, non costituendo vincolo di attuazione;

- PO: acronimo di “positivo”, nei casi in cui siano prospettati elementi valutati come conformi alla normativa e alle policy regionali in materia di protezione dei dati personali.

Nei casi in cui il DPO esprima pareri “NC” e “OS” il direttore o i dirigenti dell’ARL devono formalizzare, nelle medesime forme utilizzate dal DPO per l’espressione del parere, le motivazioni che giustificano l’esecuzione dell’attività o l’implementazione della soluzione tecnologica, in contrasto alle indicazioni fornite dal DPO. I pareri espressi dal DPO sono conservati agli atti del soggetto attuatore.

7. Il Gruppo dei referenti privacy – Funzioni e compiti

Al Gruppo di referenti, già costituito con determinazione della Regione Emilia-Romagna n. 2354/2008 e prorogato da ultimo con determinazione n. 2506/2017, fanno parte componenti dell’ARL segnalati a tal fine.

Il coordinamento del Gruppo è demandato al Servizio ICT regionale, che cura l’aggiornamento dei componenti, sulla base delle comunicazioni provenienti dalle diverse strutture.

Il Gruppo costituisce attuazione dei principi di informazione e sensibilizzazione del Regolamento europeo n. 679/2016, assicura un presidio per tutte le strutture del più ampio “sistema regionale” (di cui l’ARL fa parte ai sensi del comma 3 bis, art. 1, L.R. 43/2001) per quel che concerne gli adempimenti continuativi, lo studio e l’approfondimento degli aspetti normativi, organizzativi e procedurali, derivanti anche delle nuove disposizioni normative.

8. Disciplina dei rapporti tra DPO, l’ARL e R.P.C.T in materia accesso civico generalizzato

Con specifico riferimento alla normativa in materia di trasparenza, si ritiene opportuno disciplinare la necessaria interazione tra il DPO, l’ARL e il Responsabile per la prevenzione della corruzione e trasparenza (R.P.C.T.).

Il D.L. 97/2016, di modifica del D.lgs. 33/2013 ha introdotto l’istituto dell’accesso civico “generalizzato”, che attribuisce a “chiunque” il diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione.

L’esercizio di tale diritto soggiace ai limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall’articolo 5-bis” del d.lgs. n. 33/2013.

L’art. 5, c. 5, d.lgs. n. 33/2013 prevede che, per ciascuna domanda di accesso generalizzato, l’amministrazione debba verificare l’eventuale esistenza di controinteressati, eccetto i casi in cui la richiesta di accesso civico abbia ad oggetto dati la cui pubblicazione è prevista dalla legge come obbligatoria.

Il DPO funge da supporto alle strutture regionali competenti sulle singole richieste di accesso nella fase di individuazione dei soggetti da ritenersi controinteressati e comunque per tutti gli aspetti relativi alla protezione dei dati personali inerenti le richieste di accesso civico generalizzato.

Il DPO funge altresì da supporto al R.P.C.T. nei casi di riesame di istanze di accesso negato o differito a tutela dell’interesse alla protezione dei dati personali.

In aderenza al punto c) del paragrafo 7.2, il DPO, inoltre, su richiesta delle strutture regionali, esprime proprio parere in ordine alla valutazione dell’eventuale pregiudizio che l’accesso potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alle tutele dei loro dati personali ai sensi del comma 2 dell’art. 5-bis e, in via generale, del Regolamento UE n. 679/2016.

In aderenza al punto d) del paragrafo 7.2, il DPO, su richiesta delle strutture regionali, formula il proprio parere, entro tre giorni, in ordine all'opposizione formulata dai controinteressati nella misura in cui questa sia riferibile ad elementi afferenti alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli opponenti.

Sulla scorta di tale parere le strutture regionali competenti sulle singole richieste di accesso effettueranno il bilanciamento tra gli interessi asseritamente lesi e la rilevanza dell'interesse conoscitivo della collettività che la richiesta di accesso mira a soddisfare.

AGENZIA REGIONALE PER IL LAVORO EMILIA-ROMAGNA

ALLEGATO B

Linee guida in materia di protezione dei dati personali e sicurezza delle informazioni nell'Agenzia regionale per il lavoro dell'Emilia-Romagna

Sommario:

1. Premessa

1.1. Scopo delle linee guida

Le presenti linee guida nascono dall'esigenza di avere un insieme comune di informazioni e raccomandazioni riguardo alle operazioni di trattamento di dati personali effettuate all'interno dei servizi dell'Agenzia Regionale per il lavoro dell'Emilia-Romagna (di seguito ARL).

Il documento assolve quindi alle seguenti finalità pratiche:

- trovare risposte concrete alle problematiche più comuni di fronte alle quali possono trovarsi gli operatori dell'ARL;
- far acquisire consapevolezza in merito ad alcune criticità legate al trattamento dei dati personali;
- condividere le scelte individuate a livello direzionale per risolvere le criticità rilevate.

I titoli di paragrafi e i sotto paragrafi del documento che riportano nella dicitura articoli e considerandi si intendono sempre riferiti al regolamento UE 2016/679 (di seguito GDPR).

1.2. Ambiti considerati

Le linee guida illustrano i principi fondamentali del trattamento e della protezione dei dati personali, le principali novità introdotte dal GDPR e una prima analisi sull'applicazione nel sistema regionale lavoro. Da subito si evidenzia l'accresciuta responsabilità del titolare e del responsabile incentrata sul principio di accountability.

Accountability significa che, in forza del Regolamento, il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate a garantire, ma soprattutto, essere in grado di dimostrare, che il trattamento è stato effettuato conformemente al Regolamento. Aiutano a dimostrare la conformità del trattamento al Regolamento: la tenuta di un registro del trattamento che è obbligatorio per organizzazioni con più di 250 dipendenti, l'adesione a codici di condotta, l'applicazione eventuale di un meccanismo di certificazione che consenta di valutare rapidamente il livello di protezione dei dati personali.

Inoltre, le linee guida illustrano i principali compiti dei diversi soggetti chiamati in causa dal nuovo regolamento con alcune schede descrittive di sintesi utili a inquadrare il "chi fa cosa" dal punto di vista privacy all'interno dell'ARL.

2. Indirizzi generali

Il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio abroga la precedente direttiva 95/46/CE e detta una disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi e adempimenti a carico dei soggetti che trattano dati personali, ivi comprese le pubbliche amministrazioni. Il regolamento definisce come dato personale qualsiasi "informazione riguardante una persona fisica identificata o identificabile (interessato)".

Le disposizioni del D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" continuano a trovare applicazione, inoltre, si evidenzia che l'adeguamento della normativa nazionale alle disposizioni del regolamento è stata effettuata con il D.Lgs. 101/2018.

2.1. Che cosa cambia con il nuovo regolamento

Il Regolamento UE cambia la prospettiva con cui inquadrare la protezione dei dati personali sebbene a una prima lettura possa rispecchiare una impostazione simile a quella della precedente direttiva (c.d. Direttiva Madre) soprattutto nelle parti principali: informativa, finalità, consenso, ai ruoli, ai diritti degli interessati e ai doveri dei titolari e dei responsabili del trattamento.

Nello specifico, Il GDPR consacra il diritto alla protezione dei dati personali come diritto fondamentale e costituzionale configurandolo come diritto alla autodeterminazione informativa e,

inoltre, traccia il passaggio da un diritto alla protezione dei dati personali di tipo nazionale/individuale ad un diritto di tipo europeo/sociale.

In generale, per tutte le istituzioni pubbliche e private, il GDPR:

a) accresce le responsabilità del titolare e del responsabile con la positivizzazione del principio di accountability con la finalità di porre chi tratta i dati personali in una posizione di ridurre i rischi di operazioni non conformi o non consentite motivando, in tal senso, il titolare e il responsabile a comportamenti e prassi virtuose;

b) muta l'approccio regolatorio da "formale e reattivo" in "sostanziale e proattivo", il trattamento e la protezione dei dati personali evolvono nell'acquisire una propria e autonoma rilevanza all'interno dei processi organizzativi e gestionali dell'organizzazione;

c) consolida le garanzie e i diritti azionabili dall'interessato per il controllo delle proprie informazioni e l'esercizio dell'autodeterminazione ereditati dalla Direttiva, riaffermandone molti: diritto all'accesso, rettifica, cancellazione, limitazione, revoca e opposizione; rafforzandone altri: il consenso che diventa sempre esplicito e la trasparenza perfezionando le informazioni da esporre nell'informativa; introducendone di nuovi: diritto alla portabilità, all'oblio, all'opposizione verso il trattamento di profilazione;

d) centralizza la governance e il controllo sul rispetto e la conformità dei trattamenti alla normativa, tramite valorizzazione delle Autorità di Controllo nazionali.

2.2. Accresciuta responsabilità del titolare e del responsabile del trattamento.

La responsabilità del titolare (art. 24 e 25 GDPR) e del responsabile (art. 28 GDPR) si configura come una sostanziale assunzione di rischio, atteso che il titolare deve mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, la conformità del trattamento al regolamento tenendo conto della natura, dell'obbligo, del contesto e delle finalità di trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le liberà delle persone fisiche.

A titolari e responsabili di trattamento si affianca una nuova figura obbligatoria per le pubbliche amministrazioni: il responsabile della protezione dei dati personali (c.d. "data protection officer" - DPO).

Prioritariamente rientrano tra le responsabilità del Titolare e dei Responsabili: l'attuazione delle prassi di privacy by design/default, la valutazione d'impatto, la definizione e il mantenimento delle procedure di sicurezza e valutazione dei rischi, la tenuta dei rispettivi registri delle attività di trattamento, la valutazione prudenziale sulla violazione dei dati personali, del coefficiente di gravità e delle relative ricadute sul soggetto interessato.

2.3. Rafforzamento delle tutele riservate all'interessato

Nel nuovo Regolamento è rafforzata l'introduzione delle misure di sicurezza e delle misure di tutela e garanzia dell'interessato nel trattamento dei suoi dati, sin dalla progettazione degli strumenti utilizzati. In particolare, sono previsti i seguenti obblighi:

2.3.1 Privacy by design - considerando 78) art. 25 comma 1

Attiene le buone prassi di protezione dei dati personali sin dalla progettazione del trattamento. Le misure strumentali a tale scopo sono:

i) la migliore applicazione del principio di minimizzazione dei dati personali oggetto del trattamento con riferimento tanto alla quantità dei dati, tanto ai tempi di conservazione e ai livelli di accessibilità, tanto alle prefissate finalità;

ii) la pseudonimizzazione ovvero l'oscuramento (reversibile) dei dati identificativi del soggetto interessato;

iii) definizione di dati personali e tempi strettamente necessari al trattamento, in relazione alle diverse finalità.

2.3.2 Privacy by default - considerando 78) art. 25 comma 2

Il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita (di default), solo i dati personali necessari per ogni specifica finalità del trattamento e quindi non risultino eccedenti rispetto al ruolo del soggetto che li tratta.

Ad esempio, risulta quindi rilevante curare le diverse autorizzazioni di lettura e di modifica dei dati in relazione ai diversi profili dei soggetti autorizzati al trattamento, curando adeguatamente anche eventuali procedure organizzative interne.

2.3.3 Valutazione di impatto (DPIA) - considerando da 89 a 96, art. 35, 36

La valutazione d'impatto è volta a compensare particolari probabilità e gravità di rischio. Viene richiesta per trattamenti su larga scala, con incidenza su un vasto numero di interessati, con un elevato rischio connesso all'introduzione di nuove o particolari tecnologie, all'implementazione di trattamenti di profilazione o di sorveglianza o all'utilizzo di particolari dati (biometrici o giudiziari).

L'Autorità di controllo redige e pubblica l'elenco di tipologie di trattamenti soggetti a preventiva valutazione di impatto.

La valutazione di impatto deve contenere almeno:

- una descrizione sistematica dei trattamenti previsti, delle finalità e l'eventuale ricorrenza di un legittimo interesse;
- la valutazione sulla necessità e la proporzionalità dei trattamenti rispetto alle predefinite finalità;
- la valutazione dei rischi per i diritti e le libertà degli interessati;
- le previste misure organizzative e tecniche, comprese quelle di sicurezza, e ogni meccanismo ritenuto utile per la tutela dei diritti dei soggetti interessati.

La responsabilità della valutazione d'impatto attiene prioritariamente il Titolare. Si rende necessaria in caso di drastica revisione tecnologica, per i trattamenti di larga scala, e per i trattamenti indicati dall'Autorità di controllo.

2.3.4 Sicurezza e valutazione dei rischi - considerando 83, 84, art. 32

Il regolamento prevede misure di sicurezza idonee da adottare in relazione alla valutazione dei rischi.

Titolare e responsabile sono tenuti tanto alla valutazione dei rischi quanto all'adozione delle misure che comprendono: la pseudonimizzazione, la cifratura; misure implementative della riservatezza, dell'integrità, della disponibilità delle informazioni; la resilienza dei sistemi e delle applicazioni di trattamento nonché il loro tempestivo ripristino in caso di incidente fisico o tecnico.

Le misure vanno contemperate allo stato dell'arte, ai costi di attuazione, alla natura, al contesto e alla finalità di trattamento.

2.3.5 Violazione dei dati personali e relativa notifica - considerando da 85 a 88, art. 4, 33, 34

Il regolamento declina la violazione dei dati personali affiancando alla tradizionale componente dolosa quella accidentale.

La violazione del dato personale viene definita come 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.

Il titolare deve comunicare all'Autorità di Controllo l'avvenuta violazione dei dati personali trattati entro e non oltre 72 ore dall'acquisizione della conoscenza dell'accadimento descrivendone la natura

della violazione, le categorie e il numero approssimativo degli interessati e del numero di registrazioni dei dati personali in questione; i dati di contatto del responsabile della protezione dei dati; le probabili conseguenze della violazione; le misure adottate o che si intendono adottare per rimediare la violazione o attenuarne gli effetti negativi.

Nel caso di avvenuta violazione di dati personali riferiti a un Responsabile, tale soggetto deve informare il Titolare.

Oltre alla comunicazione all'Autorità di Controllo, la violazione deve essere comunicata anche all'interessato se la violazione è suscettibile di elevati rischi per i diritti e le libertà dell'interessato (art. 34 del GDPR).

2.3.6 Introduzione dei registri delle attività di trattamento – considerando 82, art. 30.

Il titolare e il responsabile di trattamento devono tenere i rispettivi registri delle attività.

Il registro del titolare deve contenere: riferimenti di contatto del titolare, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati; le finalità del trattamento; la descrizione degli interessati e dei destinatari; la categoria dei dati personali trattati; la presenza o meno di trasferimenti di dati verso un Paese Terzo, un'organizzazione internazionale unitamente alla documentazione sulle appropriate garanzie; la tempistica della cancellazione dei dati; la descrizione della misure di sicurezza e organizzative adottate.

Il registro del responsabile deve contenere oltre alle due ultime voci previste per il registro del titolare anche: i riferimenti di contatto dei responsabili, dei titolari per conto dei quali operano, dei rappresentanti e del responsabile della protezione dei dati; le categorie dei trattamenti effettuati per conto del titolare.

2.3.7 Smaltimento di dispositivi e supporti contenenti dati personali

Permane l'obbligo di garantire la protezione dei dati anche mediante un'accurata cancellazione al momento della distruzione dei supporti che li contengono. Sul tema, si segnala un provvedimento dell'Autorità Garante su "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali" - 13 ottobre 2008 - G.U. n. 287 del 9 dicembre 2008.

3 Diritti dell'interessato

3.1 Consenso – considerando 39, 42, 43 e art. 6, 7

Premesso che la liceità dei trattamenti dell'ARL è prevista dall'art. 6 co. 1 lettera E del GDPR, i soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali (si vedano considerando 43, art. 9 GDPR) poiché effettuati in virtù di una previsione di legge.

In generale, il consenso deve essere: libero, specifico, informato e inequivocabile; non è ammesso il consenso tacito o presunto. Deve essere reso e manifestato attraverso dichiarazione o azione positiva inequivocabile e concludente come la selezione di un'apposita casella in un sito web, la scelta di specifiche impostazioni tecniche o qualsiasi altra dichiarazione o comportamento che indichi chiaramente la volontà dell'interessato di accettare il trattamento proposto. Non è richiesta necessariamente la forma scritta anche se questa risulta essere la modalità più idonea ad accertare che il consenso sia stato inequivocabilmente fornito e che sia esplicito.

Si precisa che nel caso il trattamento richieda il consenso, il titolare dovrà essere in grado di dimostrare inequivocabilmente di averlo ottenuto.

Per il trattamento di dati sensibili, il GDPR parla di categorie particolari di dati, è necessario il consenso (art.9 comma 2 lettera a)) a meno che il trattamento non sia necessario per la tutela di diritti di grado superiore dell'interessato stesso o pubblici o di terzi, oppure per obbligo di legge, qualora l'interessato non sia in grado di fornire il consenso (art. 9 comma 2 lettere c, f, g, i, j).

3.2 Informativa – considerando da 58 a 73, art. 12, 13, 14

Il titolare del trattamento è tenuto a fornire l'informativa all'interessato, indipendentemente dall'obbligo di acquisire il consenso, salvo il caso in cui l'interessato sia già in possesso delle informazioni (art. 13 co. 4) o in altri casi particolari descritti nel regolamento (art. 14 co. 5).

Il titolare del trattamento è tenuto a informare il soggetto interessato in merito a:

- identità e dati di contatto del titolare del trattamento, del suo rappresentante e del responsabile della protezione dei dati personali;
- le finalità del trattamento cui sono destinati i dati personali;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- l'eventuale intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- i diritti azionabili dall'interessato comprendenti: l'accesso ai dati personali, la rettifica o la cancellazione degli stessi, la limitazione del trattamento o l'opposizione; oltre al diritto alla portabilità dei dati; la revoca del consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; il diritto di proporre reclamo a un'autorità di controllo;
- la necessità di comunicare i dati personali in base a un obbligo legale o contrattuale oppure se si tratta di un requisito necessario per la conclusione di un contratto, nonché la natura obbligatoria o facoltativa del conferimento, nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative circa la logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

3.3 Diritti "tradizionali" – considerando da 58 a 73, art. 12 a 17

I diritti azionabili dall'interessato, oltre a quello di ricevere idonea informativa riguardano: il diritto di accesso, la rettifica, la cancellazione, l'opposizione al trattamento.

Tra le novità previste nel nuovo GDPR abbiamo che:

- il riscontro deve essere fornito senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Nel caso di diniego, il riscontro deve essere fornito al più tardi entro un mese dal ricevimento della richiesta
- la definizione da parte del titolare di eventuali oneri gravanti sull'interessato nei casi particolari previsti nell'art. 12 comma 5.

A differenza della normativa previgente, è posto l'accento su elementi come il periodo di conservazione e le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi.

3.4 Nuovi Diritti: diritto di limitazione; diritto di opposizione alla profilazione; diritto alla cancellazione / all'oblio; diritto alla portabilità; – art. 18, 20, 21, 22

Il diritto alla limitazione rappresenta un diritto diverso e più esteso rispetto al "blocco" del trattamento già previsto dal codice, in particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento e quale alternativa alla cancellazione dei dati stessi, bensì anche nelle more che sia riscontrata, da parte del titolare, una richiesta di rettifica dei dati o di opposizione al trattamento.

Il diritto di opposizione alla profilazione che riconosce all'interessato il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare (legata ad esempio alla propria situazione economica o di salute), al trattamento dei dati personali che lo riguardano compresa la profilazione. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Il diritto "all'oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata nel caso questi siano stati resi pubblici on-line. I titolari hanno l'obbligo di informare della richiesta di cancellazione ogni altro titolare che tratta i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione".

Il diritto alla portabilità si applica ai dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato e solo per i dati che siano stati "forniti" dall'interessato al titolare; fanno eccezione quindi i dati il cui trattamento si fonda sull'interesse pubblico come quelli gestiti dall'ARL. Per tale ragione le implicazioni del Diritto di Portabilità non dovrebbero interessare i trattamenti dei dati personali nell'ARL.

3.5 Sintesi delle principali novità

Le principali novità sono sintetizzate per parole e concetti chiave nelle seguenti tabelle.

Consenso	Libero, specifico, informato, inequivocabile e concludente.
Informativa	Informazioni di contatto del titolare, rappresentante legale e DPO; indicazione della finalità di trattamento; destinatari e categorie di dati trattati; eventuale trasferimento dati personali in paesi terzi; diritti azionabili e implicazioni;
Valutazione impatto	Ripensamento delle tecnologie a supporto dei trattamenti. Analisi ed eventuale consultazione preventiva con l'Autorità Garante per le implicazioni sui diritti e le libertà delle persone. Obbligo del titolare, supportato dal DPO.
Sicurezza	Analisi dei rischi e di valutazione dell'adeguatezza delle misure tecniche e organizzative interne. Obbligo congiunto del titolare e del DPO.
Violazione dei dati	L'evento accidentale è uguale a quello dolosa.
Privacy by Design	Applicazione delle tutele di trattamento sin dalla sua progettazione e avvio. Obbligo del titolare. Impatta sui sistemi informativi
Privacy by Default	Pseudonimizzazione e Minimizzazione di dati e tempi come garanzia e misura di raggiungimento. Obbligo del titolare. Impatta su tutte le componenti della struttura organizzativa.

DPO (detto anche PDP)	Si interfaccia con il garante. Supporta titolare e responsabile del trattamento. Obbligatorio nelle PA. E' il "Garante interno all'ARL"
Registro Trattamenti	Registri di competenze in cui indicare le caratteristiche, le modalità e le finalità del trattamento. Lo redigono titolare e responsabile del trattamento. Obbligatorio per titolari e responsabili. Da esibire su richiesta del Garante.
Sanzioni	Sanzioni amministrative pecuniarie comminabili dal garante: fino a 20 000 000 EUR (per le imprese, fino al 4% del fatturato globale annuo dell'esercizio precedente)
Autorità	Comitato di controllo europeo: assicura la uniforme applicazione del Regolamento.
Autorità di Controllo	Autorità pubblica indipendente di uno Stato membro.

In merito ai nuovi diritti:

Profilazione	L'interessato ha il diritto di non subire trattamenti automatizzati (profilazione) inconsapevoli.
Portabilità dei Dati	L'interessato ha il diritto ottenere la restituzione dei propri dati personali trasmessi e trattatati da un titolare e trasmetterli ad altri. Non c'è per pubbliche amministrazioni.
Oblio	L'interessato ha diritto alla de-indicizzazione o alla cancellazione delle informazioni che lo riguardano.

4. I soggetti del trattamento

Il GDPR individua i soggetti coinvolti nel trattamento dei dati sulla base:

1) delle finalità per le quali sono raccolti:

- il Titolare è la persona giuridica o la persona fisica che raccoglie i dati personali per proprie finalità e decide i mezzi per il trattamento;
- il Contitolare è la persona giuridica o la persona fisica che condivide le finalità con altro Contitolare e stabilisce insieme a questi le modalità di trattamento;
- il Responsabile del trattamento è la persona giuridica o la persona fisica che esegue dei trattamenti di dati per conto del Titolare, sulla base di un contratto o altro atto giuridico;
- il Destinatario è la persona giuridica o la persona fisica che riceve i dati dal Titolare per eseguire i trattamenti secondo le istruzioni ricevute o che esegue trattamenti per proprie finalità, nel qual caso diventa a sua volta Titolare per i trattamenti dei dati ricevuti;
- il soggetto autorizzato è la persona fisica che ha ricevuto dal titolare precise istruzioni per l'esecuzione dei trattamenti dati di sua competenza;
- l'interessato è la persona fisica che fornisce i propri dati personali a un Titolare per le finalità specificate nell'informativa;

2) delle caratteristiche del Titolare/Responsabile e delle tipologie e quantità di dati trattati:

- il DPO è la persona giuridica o la persona fisica che segue tutti i vari aspetti relativi all'applicazione del GDPR per conto del Titolare/Responsabile, deve obbligatoriamente essere presente nelle pubbliche amministrazioni;

3) dell'ambito territoriale:

- il Rappresentante nell'Unione del Titolare/Responsabile che ha la propria sede in uno stato terzo è la persona giuridica o la persona fisica che su mandato del Titolare/Responsabile funge da interlocutore per gli interessati e per le Autorità di controllo dell'Unione (ferma restando la responsabilità generale del titolare del trattamento o del responsabile del trattamento);
- l'Autorità di Controllo è la persona giuridica pubblica istituita da ogni Stato membro per sovrintendere all'applicazione e al rispetto del GDPR nell'ambito del proprio territorio; in Italia è il Garante Privacy;
- il Comitato Europeo per la Protezione dei Dati è la persona giuridica che a livello europeo ha il compito di coordinare il lavoro delle varie Autorità di Controllo e di supportare la Commissione.

Nell'ambito dell'ARL, anche la distribuzione dei ruoli e delle responsabilità costituisce una misura di sicurezza essenziale per l'applicazione del GDPR nel rispetto del regolamento di organizzazione dell'ARL, delle linee guida di organizzazione dell'ARL e dei relativi atti di macro-organizzazione e micro-organizzazione.

4.1 Titolare del trattamento

Il titolare è definito all'art. 4 come "la 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". Pertanto, Il Titolare non viene designato o nominato ma diventa tale al momento che raccoglie dati personali con l'intento di trattarli per finalità lecite, come previsto all'art. 6, e decide le modalità di trattamento.

Soggetto del trattamento	Titolare
Persona giuridica	ARL
Carica persona fisica	Rappresentante legale dell'Ente, quindi => il direttore dell'ARL
Descrizione	Il Titolare è responsabile del rispetto del GDPR all'interno dell'ARL e deve mettere in atto tutte le misure tecniche ed organizzative necessarie a garantire la protezione dei dati personali. Per dimostrare di aver rispettato tali obblighi il Titolare mantiene un filo diretto con il DPO dell'ARL.
Informazioni	Il titolare e il suo rappresentante legale devono essere resi noti
Note	Titolare del trattamento è l'ARL nel suo complesso e non può essere infatti una persona fisica ed è individuata già nel Regolamento come "l'autorità pubblica" che determina le finalità e i mezzi del trattamento. Il Titolare risponde della corretta applicazione della normativa in materia di protezione dei dati personali.

4.2 Contitolare

La contitolarità avviene quando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento. La contitolarità quindi deve essere individuata partendo dalla definizione di Titolare del trattamento, come spiegata sopra, e quindi procedendo con il comprendere se il rapporto tra le parti in oggetto è paritario in merito al trattamento dati, oppure se vi è un rapporto gregario, in cui una delle parti è titolare e l'altra o le altre ricoprono il ruolo di responsabile del trattamento. Su entrambi i contitolari gravano le medesime responsabilità relativamente agli obblighi derivanti dalle nuove norme e dunque entrambi sono passibili delle sanzioni previste per i Titolari del trattamento.

Soggetto del trattamento	Contitolare
Persona giuridica/fisica	Può essere sia persona giuridica che fisica.
Carica/persona fisica	Rappresentante legale / persona fisica
Descrizione	Il soggetto terzo che condivide le decisioni sulle finalità per le quali trattare i dati e che contribuisce a definire le modalità di trattamento. Potrebbe essere il soggetto che insieme all'ARL collabora al raggiungimento di finalità condivise.
Informazioni per l'interessato	Il contenuto essenziale dell'accordo stipulato fra i contitolari deve essere reso noto all'interessato. Questi può esercitare i propri diritti nei confronti di ogni contitolare.

4.3 Responsabile del trattamento dati

Il GDPR definisce all'art. 4 il Responsabile del trattamento quale "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento" e ne descrive le funzioni all'art.28. Differisce dalla figura di responsabile prevista dall'attuale Codice, soprattutto per quanto concerne il rispondere in solido con il Titolare di eventuali inadempienze. Con il GDPR il responsabile del trattamento dati è attribuito a soggetti esterni che eseguono trattamenti di dati per conto dell'ARL. Certamente è necessario che l'ARL, quale Titolare, mantenga al proprio interno una distribuzione delle responsabilità rispetto al trattamento dati, "istruendo" opportunamente le persone a partire da quelle che dirigono i servizi, affinché si facciano carico dell'applicazione del GDPR nel proprio ambito, collaborando con il Titolare e con il DPO. La definizione di un'organizzazione interna finalizzata all'attuazione e al controllo efficace delle misure adottate per la protezione dei dati da parte del Titolare è un elemento fondamentale per poter dimostrare che il trattamento è effettuato conformemente al GDPR. Pertanto, per l'applicazione di tale disposizione risulta utile distinguere fra la funzione di "Responsabile del trattamento", così come definita all'art.28 del GDPR, assegnata a un soggetto esterno che esegue trattamenti e la funzione che possiamo definire di "Responsabile interno delegato all'attuazione" che è assegnata a personale che ricopre funzioni di particolare rilievo organizzativo (in genere i dirigenti dell'ARL). Il responsabile esterno agisce come persona giuridica/fisica autonoma e quindi risponde in solido con il titolare di eventuali inadempienze, mentre il responsabile interno agisce per conto del titolare all'interno dell'ARL sulla base del ruolo organizzativo ricoperto. Il Responsabile del trattamento sarà quindi sempre un soggetto esterno all'ARL.

Soggetto del trattamento	Responsabile del trattamento dati
Persona giuridica/fisica	Soggetto esterno
Carica/persona fisica	Rappresentante legale/persona fisica
Descrizione	Il responsabile del trattamento dati è un soggetto esterno che esegue, in base a un contratto/convenzione o altro atto giuridico, dei trattamenti di dati personali per conto del titolare e ne risponde in solido in caso di inadempienze (es. Ervet). Al Responsabile spettano tutti i compiti del Titolare all'interno del proprio organismo (valutazione impatto, registro dei trattamenti, eventuale nomina del Responsabile della Protezione Dati, ecc.). Il Responsabile così individuato non può a sua volta nominare un altro Responsabile se non dietro autorizzazione scritta del Titolare: in ogni caso la catena delle responsabilità deve essere nota al Titolare. Nei contratti con sub-responsabili devono essere riportati gli stessi obblighi in materia di protezione dei dati personali previsti dal contratto tra responsabile e titolare.
Informazioni per l'interessato	Nell'informativa devono essere indicati i destinatari o le categorie di destinatari ai quali sono comunicati i dati per il loro trattamento.

Note	Rientrano in questa categoria i soggetti che, per esempio, curano le applicazioni in outsourcing o in hosting per conto dell'ARL. Quantomeno nella fase di stipula del contratto, devono essere predisposte clausole specifiche che indichino gli ambiti di responsabilità e i compiti assegnati. Il responsabile a sua volta deve garantire l'applicazione delle misure necessarie alla protezione dei dati e gli adempimenti previsti dal Regolamento. Al punto 5 dell'art. 28 è previsto che possono essere considerate garanzie sufficienti per la protezione dei dati l'adesione da parte del responsabile a codici di condotta o certificazioni approvate secondo quanto stabilito agli artt. 40 e 42 del GDPR. In caso di designazione di un sub-responsabile il responsabile conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del sub- responsabile.

4.4 Soggetti autorizzati (i vecchi incaricati)

Nelle linee guida del Garante (https://www.garanteprivacy.it/regolamentoue/titolare-responsabile-incaricato-del-trattamento) si afferma che "le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del regolamento", ne consegue che quanto disposto all'art. 29 del GDPR possa concretizzarsi con l'individuazione con atto formale dei soggetti autorizzati al trattamento dati all'interno dell'ARL, prima denominati "incaricati", anche se la nuova impostazione dal taglio sostanziale voluta dal GDPR tenderebbe a fare prevalere la ricostruzione "de facto" del ruolo a partire dall'assetto organizzativo e l'obbligo di istruirli. Si sottolineata l'importanza di "istruire" i soggetti, sarà quindi opportuno prevedere leve formative adeguate per coloro che saranno coinvolti nel trattamento dati. Le presenti linee guida sono altresì una azione di istruzione per gli autorizzati.

Soggetto autorizzato del trattamento	Soggetti "istruiti" dal Titolare per trattare dati
Persona fisica	Soggetto interno/esterno
Carica/persona fisica	Personale dipendente o collaboratori
Descrizione	Il GDPR non prevede espressamente la figura dell'incaricato del trattamento, ma all'art. 29 prescrive che l'accesso ai dati personali e i loro trattamenti devono essere effettuati da soggetti "istruiti" (in inglese è "on instructions") dal Titolare. Tale affermazione non esclude tuttavia che all'interno dell'ARL possano essere individuati coloro che sono autorizzati a effettuare i trattamenti, così come suggerito dal Garante Privacy nella guida http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento- europeo-in-materia-di-protezione-dei-dati-personali. A tale scopo può essere individuata una organizzazione funzionale alla protezione dei dati, nella quale si delineano i vari ambiti di trattamento che competono ad ogni struttura e l'individuazione dei soggetti "incaricati" dei trattamenti secondo le afferenze, le mansioni e le responsabilità.

Informazioni per l'interessato	Nell'informativa devono essere indicati i destinatari o le categorie di destinatari, anche interni, ai quali sono comunicati i dati per il loro trattamento.
Note	In linea teorica, stante quanto sopra descritto e analogamente a quanto è stato fatto fino ad oggi, è possibile individuare i soggetti che sono autorizzati al trattamento dei dati, mediante una nomina individuale da parte del Titolare o Responsabile del trattamento dati, oppure, in linea pratica, si potrebbe procedere individuando i trattamenti che competono all'unità organizzativa di afferenza del soggetto, che risulta pertanto incaricato per "documentata preposizione ad unità organizzativa".

4.5 DPO - Responsabile della protezione dati

Il GDPR definisce all'art. 28 le funzioni del DPO che fornisce il proprio parere in ordine alla legittimità e alla correttezza dei trattamenti di dati personali eseguiti dall'ARL.

Soggetto del trattamento	Data Protection Officer
Persona giuridica/fisica	Soggetto interno/esterno
Carica	Persona fisica/giuridica con incarico specifico
Descrizione	L'incarico può essere affidato a personale interno o a soggetto esterno, verificando che non vi siano conflitti d'interesse. A seconda della complessità e della quantità di dati trattati, può essere individuato un team di persone che svolgono tale funzione, purché siano ben definite le mansioni e le responsabilità al suo interno. Diversamente la funzione di DPO può essere svolta per più organismi dalla stessa persona, nel caso che non sia previsto un impegno a tempo pieno. Il DPO agisce in autonomia in quanto non riceve alcuna istruzione per quanto riguarda l'esecuzione di tali compiti e funge da collegamento fra Titolare/Responsabile, gli interessati e l'autorità di controllo. I suoi compiti devono essere chiaramente definiti e devono essergli garantiti supporto, risorse e tempi di lavoro adeguati allo svolgimento della sua funzione. Nel caso di personale interno deve inoltre essergli garantita una formazione permanente per permettergli di rimanere aggiornato sugli sviluppi nel settore della protezione dei dati. Al DPO deve essere dato ampio accesso alle informazioni e deve essere interpellato per ogni problematica inerente la protezione dei dati e per ogni attività che implica un trattamento dati, fin dalla sua progettazione. Il DPO ha il compito di coadiuvare il Titolare/responsabile nella valutazione d'impatto e nella redazione del Registro dei Trattamenti, oltre che nella sorveglianza del rispetto del GDPR all'interno dell'ARL. Informa e fornisce consulenza sull'applicazione del GDPR al Titolare/Responsabile e al personale interno coinvolto nel trattamento dati. Si occupa delle comunicazioni con l'autorità di controllo e con gli interessati. Nell'assolvimento dei suoi compiti il DPO non può essere penalizzato o rimosso. Le eventuali osservazioni del DPO sull'applicazione del GDPR possono essere non accolte dal

	Titolare/Responsabile, specificandone i motivi. La responsabilità di eventuali mancanze è comunque a carico del solo Titolare/Responsabile. Il DPO deve essere facilmente contattabile dal personale interno, dagli interessati e dall'autorità di controllo. Pertanto i suoi recapiti (è consigliato indicare anche il nominativo, ma non è obbligatorio) devono essere ampliamente pubblicizzati.
Informazioni per l'interessato	I recapiti del DPO devono essere forniti all'interessato nell'informativa.
Note	Sul sito del Garante sono pubblicate delle linee guida specifiche per tale figura (http://www.garanteprivacy.it/rpd).

4.6 Destinatario

Il GPDR all'art. 4 definisce destinatario "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi". I destinatari o le categorie di destinatari ai quali verranno comunicati i dati devono essere definiti in fase di raccolta dei dati per inserirli nell'informativa all'interessato. Nel caso che il destinatario sia un soggetto che risiede in un paese non membro dell'Unione, è richiesto che il Titolare verifichi che le garanzie offerte da questi per la protezione dei dati siano adeguate.

Soggetto del trattamento	Destinatario
Persona giuridica/fisica	Soggetto interno/esterno, persona fisica, persona giuridica
Carica/persona fisica	Rappresentante legale, persona fisica
Descrizione	Il destinatario è il soggetto al quale sono comunicati i dati personali da parte di un titolare.
Informazioni per l'interessato	Nell'informativa da fornire all'interessato devono essere indicati i destinatari o le categorie di destinatari ai quali saranno comunicati i dati.
Note	Nel caso il destinatario sia un soggetto "terzo" che riceve i dati per perseguire proprie finalità, diventerà a sua volta titolare. Per esempio, l'ARL comunica dati personali di lavoratori a soggetti esterni che svolgono attività di ricerca e selezione di personale per l'inserimento nel mondo del lavoro. Il destinatario che riceve i dati da altro titolare per perseguire finalità proprie è tenuto a dare l'informativa all'interessato nel più breve tempo possibile, sempre che ciò non sia impossibile o richieda uno sforzo sproporzionato.

4.7 Interessato

L'interessato è il soggetto "proprietario" dei dati personali e su questi conserva dei diritti nei confronti del titolare del trattamento. Il GDPR al Capo III elenca nel dettaglio tali diritti che sono stati descritti nei paragrafi precedenti. Alcuni di questi, a seconda della finalità per la quale i dati sono stati raccolti, potrebbero non essere esercitabili dagli interessati. Per esempio, non è possibile effettuare la cancellazione dei dati relativi alla carriera di un dipendente dell'ARL perché devono essere conservati illimitatamente per pubblico interesse, mentre può essere accolta la richiesta di cancellazione dei recapiti personali ma solo dopo la cessazione del rapporto di lavoro.

La risposta alle richieste dell'interessato deve comunque essere tempestiva e, anche nel caso non sia possibile soddisfarla, occorre specificare la motivazione del rifiuto. Il titolare ha il compito di facilitare l'accesso all'interessato ai suoi dati, predisponendo dei canali di comunicazione dedicati, quali ad esempio i recapiti del Responsabile della Protezione dei Dati.

Per la descrizione dei trattamenti si usa raggruppare gli interessati in categorie omogenee a seconda del tipo di rapporto che questi hanno con il titolare. A titolo esemplificativo si possono individuare le seguenti principali categorie d'interessati, le quali possono poi essere suddivise in sottocategorie per distinguerle all'interno di alcuni trattamenti:

- Personale;
- Collaboratori;
- Fornitori;
- Cittadini utenti dei servizi;
- Privati cittadini.

4.8 Autorità di controllo e comitato europeo

Le autorità di controllo sono incaricate di "sorvegliare l'applicazione del presente GDPR al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione" (punto 1) art. 51 del GDPR.

Ogni stato membro istituisce una o più autorità pubbliche indipendenti. Nel caso siano più di una deve essere designata quella che le rappresenterà nel Comitato europeo per la protezione dei dati, che ha funzioni di coordinamento delle varie autorità di controllo, per rendere coerenti e in linea con il GDPR le varie decisioni che a queste competono. Il Comitato ha inoltre funzioni di supporto per la Commissione europea. All'Autorità di controllo nazionale devono essere comunicati eventuali data breach. Le Autorità di controllo sono competenti ad accogliere e decidere su eventuali reclami presentati dagli interessati.