



UNIVERSITÀ DI PARMA

ISTRUZIONI FUNZIONALI AL TRATTAMENTO DI DATI PERSONALI ai sensi dell'art. 29 del GDPR e dell'art. 2 quaterdecies del D.lgs. 196/2003 e s.

Oggetto: autorizzazione al trattamento dati comprensiva di istruzioni funzionali rivolte al personale e ai collaboratori che agiscono sotto l'autorità del Titolare del trattamento, ai sensi e per gli effetti dell'art. 29 del 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 (General Data Protection Regulation - "GDPR") e dell'art. 2 quaterdecies del D.lgs. 196/2003 e s.m.i.

PREMESSO CHE

- L'articolo 29 del GDPR dispone che: *"Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri"*.
- L'articolo 32 del GDPR ribadisce che: *"Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri"*.
- L'articolo 2 quaterdecies del Codice Privacy (D.lgs. 196/2003, come armonizzato al GDPR dal D.lgs. 101/2018) intitolato "Attribuzione di funzioni e compiti a soggetti designati" dispone che:
"1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.
2. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta".
- Il principio generale di "accountability" / "responsabilizzazione" previsto dall'articolo 24 del GDPR, dispone che il titolare del trattamento dei dati, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR.
- Si intende per:

- **Dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile ("**interessato**"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un nome di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **Categorie particolari di dati:** dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
- **Dati personali relativi a condanne penali e reati:** dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;
- **Archivio (banca dati / database):** qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- **Trattamento:** qualunque operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- **Comunicazione:** il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel



UNIVERSITÀ DI PARMA

- territorio dell'Unione europea, dalle persone autorizzate, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
- **Diffusione:** il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
 - **Consenso dell'interessato:** qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
 - **Profilazione:** qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
 - **Pseudonimizzazione:** il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
 - **Autorità Garante / Garante privacy o semplicemente il "Garante":** si intende l'Autorità Garante per la protezione dei dati personali, istituita dalla L. 675 del 31/12/1996 e di cui all'art. 153 del Codice Privacy armonizzato;
 - **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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
 - **Responsabile del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
 - **Destinatario:** la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
 - **Amministratore di sistema:** figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali;
 - **Autorizzato / designato al trattamento:** chiunque acceda a determinate informazioni per svolgere specifici compiti e funzioni connessi al trattamento di dati personali sotto l'autorità del Titolare del trattamento o del Responsabile del trattamento (art. 29 GDPR e 2-quaterdecies D.lgs. 196/2003 armonizzato);
 - **Utente:** tutti i lavoratori dipendenti, i collaboratori occasionali e i consulenti che si avvalgono degli strumenti aziendali, nonché tutto il personale che - a qualsiasi titolo - presti la propria attività lavorativa, anche saltuaria e/o consulenziale, presso il Titolare, o che, per ragioni connesse all'espletamento del proprio lavoro, risulti comunque autorizzato all'uso, anche solo occasionale e/o temporaneo, delle risorse informatiche;
 - **Responsabile della Protezione dei Dati personali (RPD/DPO):** il DPO, figura storicamente già presente in alcune legislazioni europee, rappresenta un elemento fondante ai fini della responsabilizzazione, facilita l'osservanza della normativa e il margine competitivo delle imprese (si rinvia alla sez. 4 del GDPR e alle Linee guida del WP29 - WP243);
 - **Accountability:** il principio di responsabilizzazione, insieme alle altre norme che disciplinano in modo più specifico le modalità di adempimento del GDPR e la ripartizione delle responsabilità, rende necessario definire i diversi ruoli dei vari soggetti coinvolti in un'attività di trattamento di dati personali;
 - **Violazione dei dati personali (Data Breach):** 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;
 - **Sistema informativo:** insieme ordinato di elementi diversi che raccolgono, elaborano, scambiano e archiviano dati relativi a fenomeni economici e attività gestionali dell'azienda con lo scopo di produrre e distribuire informazioni nel momento e nel luogo adatto ai soggetti (in azienda) che ne hanno bisogno per la loro attività;
 - **Personal Computer (PC):** con Personal Computer si fa riferimento sia ai computer desktop/fissi che ai computer portatili notebook/laptop;
 - **Antivirus/antimalware:** software finalizzato a prevenire, rilevare ed eventualmente rendere inoffensivi codici dannosi e malware per PC come virus, adware, backdoor, BHO, dialer, fraudtool, hijacker, keylogger, LSP, rootkit, spyware, trojan, worm o ransomware.

CIÒ PREMESSO

Nell'ambito dello svolgimento delle funzioni lavorative che sono e che saranno assegnate al personale e ai collaboratori di Università degli Studi di Parma (di seguito anche l' "organizzazione"), gli stessi vengono necessariamente a conoscenza dei contenuti delle banche dati presenti all'interno dell'organizzazione (cartacee e informatiche).

UNIVERSITÀ DEGLI STUDI DI PARMA

Via Università, 12 - 43121 Parma - www.unipr.it

C.F. e P.IVA 00308780345



UNIVERSITÀ DI PARMA

Con la presente l'organizzazione intende quindi fornire, al personale e ai propri collaboratori, le istruzioni che questi dovranno necessariamente seguire, nell'esecuzione delle mansioni assegnate, per garantire un trattamento conforme alle norme.

Le istruzioni si suddividono in regole generali, universalmente applicabili, derivanti direttamente dal sopracitato Regolamento (GDPR) e in regole di dettaglio, che dipendono dalla mansione e dalle specifiche banche dati a cui viene conferito l'accesso.

REGOLE GENERALI

Il trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità previste dall'organizzazione e seguendo i principi di cui all'Articolo 5 del GDPR.

Principi applicabili al trattamento di dati personali

I dati personali devono essere:

- a) *trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);*

Assicurarsi che il trattamento sia lecito significa che ogni trattamento deve trovare fondamento in un'idonea base giuridica. I fondamenti di liceità del trattamento di dati personali sono indicati all'articolo 6 del Regolamento: consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati. Per quanto riguarda la base giuridica del trattamento di eventuali categorie particolari di dati personali e eventuali dati relativi a condanne penali e reati e connesse misure di sicurezza, si rinvia, rispettivamente, agli articoli 9 e 10 del Regolamento. Il principio di correttezza e di trasparenza si traduce nella necessità di fornire agli interessati le informazioni essenziali per comprendere il trattamento svolto dal titolare e per consentire agli stessi di esercitare i diritti previsti dal Regolamento (articoli 15-22).

- b) *raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; iniziali («limitazione della finalità»);*

Le finalità specifiche del trattamento dei dati personali devono quindi essere esplicite, legittime e precisate al momento della raccolta. Questo principio deriva dalla necessità di regolamentare la frequente utilizzazione (soprattutto in ambienti online) di dati per scopi ulteriori e incompatibili rispetto alle finalità per i quali sono stati raccolti. Trattamenti ulteriori possono essere svolti, senza la necessità di un consenso specifico o di ricorrere ad una distinta base giuridica, solo per le finalità riportate nella lettera b), ovvero "archiviazione nel pubblico interesse, ricerca scientifica o storica o fini statistici".

- c) *adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);*

Al principio di minimizzazione è possibile ricondurre i concetti di necessità e di pertinenza: devono essere trattati solo i dati strettamente necessari allo specifico trattamento. Inoltre, grazie all'utilizzo di specifiche tecnologie, talvolta è possibile evitare del tutto l'utilizzo dei dati personali: il titolare quindi, ove possibile, dovrebbe preferire la raccolta di dati anonimi / aggregati oppure di dati pseudonimizzati, che non consentano la re-identificazione dell'interessato.

- d) *esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);*

Per garantire il rispetto di questa disposizione, è opportuno adottare tutte le misure ragionevoli affinché i dati personali siano esatti e aggiornati, e affinché i dati inesatti siano rettificati o cancellati.

- e) *conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati («limitazione della conservazione»);*

Il principio della limitazione della conservazione significa che i dati personali devono essere cancellati o anonimizzati non appena questi non siano più necessari alle finalità per cui sono stati raccolti. A tal fine, il considerando 39 prevede che "il



UNIVERSITÀ DI PARMA

titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica”, per garantire che i dati non siano conservati più a lungo del necessario.

- f) trattati in maniera da garantire un’adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Il principio di integrità e riservatezza è strettamente connesso con l’art. 32 del Regolamento e si traduce nella necessità di adottare misure di sicurezza tecniche e organizzative adeguate a proteggere i dati. Tali misure devono essere implementate tenendo conto “dello stato dell’arte e dei costi di attuazione, nonché della natura, dell’oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche”.

Rinvio

Per completezza si rinvia alle principali fonti applicabili in materia di protezione dei dati personali, raggiungibili attraverso i collegamenti riportati a seguire. Gli autorizzati / designati che vogliono approfondire gli aspetti trattati nelle presenti istruzioni funzionali, possono consultare, in particolare, le schede informative tematiche pubblicate sul sito dell’Autorità Garante per la protezione dei dati personali.

- Il Regolamento europeo: <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679>
- Il sito web del Garante per la protezione dei dati personali: <https://www.garanteprivacy.it/home>, le infografiche, i vademecum e le schede divulgative, di cui, fra tutte, si ricordano le seguenti:
 - Guida all’applicazione del Regolamento europeo (<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6807118>);
 - Attenzione al ransomware. Il programma che prende "in ostaggio" il tuo dispositivo (<https://www.garanteprivacy.it/temi/cybersecurity/ransomware>);
 - Phishing: attenzione ai «pescatori» di dati personali (<https://www.garanteprivacy.it/temi/cybersecurity/phishing>);
 - Smishing: i suggerimenti del Garante per proteggersi dal phishing che sfrutta SMS e messaggistica (<https://www.garanteprivacy.it/temi/cybersecurity/smishing>);
 - Vishing: i suggerimenti del Garante per proteggersi dal phishing telefonico (<https://www.garanteprivacy.it/temi/cybersecurity/vishing>);
 - Suggerimenti per creare e gestire password a prova di privacy (<https://www.garanteprivacy.it/temi/cybersecurity/password>).

REGOLE DI DETTAGLIO

MANSIONE / FUNZIONE / RUOLO	
CATEGORIE DI DATI TRATTATI	<input type="checkbox"/> Dati personali <input type="checkbox"/> Dati particolari <input type="checkbox"/> Eventuali Dati giudiziari
CATEGORIE DI INTERESSATI COINVOLTI	<input type="checkbox"/> Clienti <input type="checkbox"/> Potenziali clienti <input type="checkbox"/> Fornitori <input type="checkbox"/> Potenziali fornitori <input type="checkbox"/> Dipendenti <input type="checkbox"/> Candidati <input type="checkbox"/> Collaboratori <input type="checkbox"/> Utenti <input type="checkbox"/> Visitatori <input type="checkbox"/> Altro (specificare) _____
TIPOLOGIA DI TRATTAMENTI AUTORIZZATI	<input type="checkbox"/> la raccolta, <input type="checkbox"/> la registrazione, <input type="checkbox"/> l'organizzazione,



UNIVERSITÀ DI PARMA

	<input type="checkbox"/> la strutturazione, <input type="checkbox"/> la conservazione, <input type="checkbox"/> l'adattamento o la modifica, <input type="checkbox"/> l'estrazione, <input type="checkbox"/> la consultazione, <input type="checkbox"/> l'uso, <input type="checkbox"/> la comunicazione mediante trasmissione, <input type="checkbox"/> diffusione o qualsiasi altra forma di messa a disposizione, <input type="checkbox"/> il raffronto o l'interconnessione, <input type="checkbox"/> la limitazione, <input type="checkbox"/> la cancellazione o la distruzione.
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Accesso agli archivi

In base al principio di stretta pertinenza dei trattamenti rispetto alle mansioni svolte, il personale autorizzato / designato potrà accedere agli archivi informatizzati e cartacei relativi alle categorie di dati sopra individuati.

Creazione nuove banche dati

Senza preventiva autorizzazione della direzione non è permesso realizzare nuove ed autonome banche dati, con finalità diverse da quelle già previste.

Comunicazione e diffusione dei dati

In relazione alle banche dati di cui è autorizzato il trattamento nello svolgimento delle mansioni affidate, ogni ipotesi di comunicazione dovrà avvenire nel rispetto delle informative fornite agli interessati e secondo le indicazioni del titolare.

La diffusione dei dati dovrà essere preventivamente autorizzata di volta in volta dal Titolare del trattamento. Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dei dati dovranno essere osservati anche in seguito a modifica dell'incarico/ruolo e/o cessazione del rapporto di lavoro.

Misure di sicurezza

Ogni soggetto autorizzato / designato al trattamento dei dati è tenuto ad osservare tutte le misure di protezione e sicurezza atte ad evitare i rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito, già predisposte dall'organizzazione, nonché quelle che in futuro verranno implementate e comunicate.

Regole per l'attività di marketing diretto, newsletter e comunicazioni commerciali

Il trattamento dei dati personali ai fini di marketing diretto deve essere effettuato in conformità al Regolamento UE 2016/679 e in base alla normativa nazionale di riferimento sul marketing (fra cui si citano, in particolare, gli artt. 121 e ss. del Codice in materia di protezione dei dati personali e le "Linee guida in materia di attività promozionale e contrasto allo spam" del Garante per la protezione dei dati personali).

Si precisa che, per poter inviare comunicazioni promozionali e materiale pubblicitario tramite sistemi automatizzati (telefonate preregistrate, e-mail, fax, sms o altri strumenti) è necessario aver prima acquisito il consenso dei destinatari (cosiddetto opt-in). Tale consenso deve essere specifico, libero, informato e documentato per iscritto. Un consenso distinto e dotato di tali caratteristiche, è richiesto anche in caso di cessione a terzi di dati personali per finalità di marketing. In tal caso, il Titolare deve previamente rilasciare agli interessati un'adeguata informativa che individui, oltre agli elementi indicati nella norma, anche ciascuno dei terzi o, in alternativa, le categorie (economiche o merceologiche) di appartenenza degli stessi (ad esempio: "finanza", "editoria", "abbigliamento", etc.).

Regole per il trattamento di categorie particolari di dati

Qualora le mansioni del soggetto autorizzato / designato comportassero il trattamento di "categorie particolari di dati personali" (articolo 9 del Regolamento), si ricorda che il loro trattamento è vietato, in prima battuta, a meno che il titolare possa dimostrare di soddisfare almeno una delle condizioni fissate all'articolo 9, paragrafo 2 del Regolamento, che qui ricordiamo:

- ✓ l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
- ✓ il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
- ✓ il trattamento è necessario per uno dei seguenti scopi:
 - per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
 - per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;



UNIVERSITÀ DI PARMA

- per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri;
- per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali;
- per motivi di interesse pubblico nel settore della sanità pubblica;
- per il perseguimento di fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Per alcune di tali finalità sono previste limitazioni o prescrizioni ulteriori, anche nel diritto nazionale.

Regole per il trattamento di dati relativi a condanne penali e reati

Qualora le mansioni del soggetto autorizzato / designato comportassero il trattamento di “dati personali relativi a condanne penali e reati” (articolo 10 del Regolamento), si ricorda che il loro trattamento, sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

Regole per il trattamento dei dati di candidati e dipendenti

Il trattamento dei dati personali ai fini della selezione e della gestione del personale deve essere effettuato in conformità al Regolamento UE 2016/679 e in base alla normativa nazionale di riferimento (fra cui si citano, in particolare, gli artt. 111 e ss. del Codice in materia di protezione dei dati personali, le “Linee guida sul trattamento di dati personali dei lavoratori privati” e l'autorizzazione generale 01/2016, al trattamento dei dati sensibili nei rapporti di lavoro, del Garante per la protezione dei dati personali).

Nell'esecuzione delle mansioni affidate al soggetto autorizzato / designato, lo stesso dovrà rispettare anche la normativa giuslavoristica strettamente connessa alla disciplina sulla tutela dei dati personali, in particolare l'art. 8 dello Statuto dei Lavoratori (Divieto di indagini sulle opinioni) che prevede “È fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore”.

Per quanto non precisato all'interno della presente lettera di incarico, si rinvia alle ulteriori istruzioni fornite al personale e ai collaboratori mediante il Regolamento sul corretto utilizzo degli strumenti aziendali, nonché mediante tutte le altre policy impattanti sulla protezione dei dati personali trattati all'interno dell'organizzazione.

Fra queste si ricordano, in particolare:

- La Data Breach Policy;
- La Data Retention Policy;
- La Procedura per l'esercizio dei diritti degli interessati;
- La Procedura da attuare in caso di ispezioni;
- La Policy in materia di Whistleblowing;
- L'Organigramma e funzionigramma privacy
- Altro (specificare) _____

Tali documenti sono reperibili in bacheca o nella intranet aziendale e sempre disponibili scrivendo a privacy@_____

Titolare del trattamento, ai sensi degli articoli 4 e 24 del Regolamento (UE) 2016/679 (GDPR) è **Università degli Studi di Parma**, con sede in via Università 12, 43121 Parma (PR), Italia, nella persona del suo Legale Rappresentante pro-tempore, che potrà contattare per qualsiasi informazione tramite: telefono: +39 0521 902111, e-mail: protocollo@unipr.it, pec: protocollo@pec.unipr.it.



UNIVERSITÀ DI PARMA

Luogo e data: _____, ____/____/____

TITOLARE DEL TRATTAMENTO

UNIVERSITA' DEGLI STUDI DI PARMA
Il Rettore

(timbro e firma)

AUTORIZZATO / DESIGNATO AL TRATTAMENTO

Nome e cognome

_____, ____/____/____
Luogo e data di nascita

Firma per presa visione e accettazione