REGISTRO DEI TRATTAMENTI DEL COMUNE DI CASTENASO

1. Contrassegno dell'attività di trattamento effettuate

RACCOLTA	CONSERVAZIONE	STRUTTURAZIONE	CONSULTAZIONE	ESTRAZIONE	COMUNICAZIONE	RAFFRONTO	INTERCONNESSIONE	CANCELLAZIONE	DIS-TRUZIONE	PSEUDOANONIMIZZAZIONE	REGISTRAZIONE	UTILIZZAZIONE
R	CSV	STR	CON	EST	CMN	RAF	INT	CANC	DIS	PSEU	REG	UT

2. Descrizione sintetica dell’attività di trattamento effettuata

- La **raccolta** dei dati è la prima operazione e generalmente rappresenta l'inizio del trattamento. Consiste nell'attività di acquisizione del dato.
- La **registrazione** consiste nella memorizzazione dei dati su un qualsiasi supporto.
- La **strutturazione** consiste nell'attività di distribuzione dei dati secondi schemi precisi.
- La **conservazione** consiste nel mantenere memorizzate le informazioni su un qualsiasi supporto.
- La **consultazione** è la mera lettura dei dati personali. Anche la mera visualizzazione dei dati è un trattamento che può rientrare nell'operazione di consultazione.
- L'**estrazione** consiste nell'attività di estrapolazione di dati da gruppi già memorizzati.
- Il **raffronto** è un'operazione di confronto tra dati, sia un conseguenza di elaborazione che di selezione o consultazione.
- L'**utilizzo** è un'attività generica che ricopre qualsiasi tipo di impiego dei dati.
- L'**interconnessione** consiste nell'utilizzo di più banche dati, e si riferisce all'impiego di strumenti elettronici.
- La **comunicazione** (o cessione) consiste nel dare conoscenza di dati personali ad uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati. In caso di comunicazione il dato viene trasferito a terzi, ed è quindi attività particolarmente delicata.
- La **cancellazione** consiste nell'eliminazione di dati tramite utilizzo di strumenti elettronici.
- La **distruzione** consiste nella eliminazione definitiva dei dati.

3.Coordinate del titolare del trattamento (art.24)

Soggetto: ***COMUNE DI CASTENASO***

Sede: ***Piazza Raffaele Bassi, n. 1 - 40055 Castenaso (BO),***

C.F. 01065340372 - P.Iva: 00531431203

PEC *comune.castenaso@cert.provincia.bo.it* ***raggiungibile per ogni comunicazione o richiesta in merito ai propri dati anche all'indirizzo e-mail*** *privacy@comune.castenaso.bo.it* ***per le disposizioni di cui al Regolamento 2016/679 e al D.Lgs. 101/18.***

Legale Rappresentante: ***il Sindaco eletto e in carica***

4. Coordinate del contitolare del trattamento, se appropriato (art. 26)

non esiste un contitolare

5. Coordinate del Responsabile del trattamento se designato (art. 28)

Responsabili del Trattamento sono le singole Posizioni Organizzative per i procedimenti di competenza, in particolare:

Area	Nominativo
Segretario Generale	Dott.ssa Letizia Ristauri
Sviluppo organizzativo e Affari Generali	Dott.ssa Maria Ottavia Chiarini
Innovazione e Servizi al Cittadino	Dott.ssa Chiara Bergamini
Bilancio, Controllo di Gestione, Tributi	Dott.ssa Monica Bonori
Servizi di Comunità	Dott.ssa Martina Masi
Tecnica e Patrimonio	Dott.ssa Silvia Malaguti
Polizia Locale	Comandante Cristina Bignami

6. Coordinate di eventuali altri responsabili esterni del trattamento, coinvolti nel trattamento stesso (art. 28)

Seguono tutti i soggetti responsabili esterni per attività in *out-sourcing suddivisi per aree di competenza professionale e i relativi contratti*

- **ASSISTENZA FISCALE**

Soggetto: Dott. Alessandro Garzon

Sede: Porto Mantovano (MN) – via Spinelli n. 6/F - CF: GRZLSN58M23C059M

- **CONSULENZA E ASSISTENZA LEGALE**

Soggetto: Studio Legale Lecchi

Sede: Bologna, Viale Risorgimento n. 7

- **MEDICO DEL LAVORO**

Soggetto: Dottor Giuseppe Pilato

Sede: via G.B. Casti, n. 17 – 47900 Rimini

- **SERVER FARM E DATA CENTER - SICUREZZA INFORMATICA**

Soggetto: Lepida S.c.p.A. - CF e P.IVA: 02770891204

Sede: via della Liberazione, 15 - Bologna

- **MANUTENZIONE E PRIMO INTERVENTO HARDWARE E SOFTWARE**

Soggetto: AdiMatica di Andrea del Monte - P.IVA 03067071203

Sede: via della Cooperazione, n. 4 – Pianoro (BO)

- **CONSULENTE DEL LAVORO:**

Soggetto: Studio Giallo Srl

Sede: Porto Mantovano (MN) – via Spinelli n. 6/F – CF e P.IVA: 02025210200

- **RSPP**

Soggetto: Dott.ssa Emanuela Tufariello Sidel Ingegneria S.r.l. c/o Sidel Ingegneria S.r.l.

Sede: Bologna, via Larga n. 36 – CF e P.IVA: 03408321200

- **ISTITUTO COMPRENSIVO DI CASTENASO**

Sede: Castenaso (BO), via Marconi 3/2 C.F. E P.IVA. 80073190375 - Legale Rappresentante: Dirigente Scolastico in carica;

- **SOCIETA' CHE EFFETTUA LA VIDEOSORVEGLIANZA;**

fino al 31/12/23 - Ditta SITE SPA con sede legale a Bologna in Via Del Tuscolano, 15 - P.IVA 03983200373,

dal 01/01/2024 - 2026 sarà la ditta ALMA SICUREZZA S.r.l., con sede in Via Palazzetti 5/F a San Lazzaro di Savena (BO), Codice Fiscale e Partita IVA 03306291208, Legale Rappresentante: Marzocchi Alberto

- **SOCIETA' CHE EFFETTUA RIMOZIONE DEGLI AUTOVEICOLI:**

1) Ditta BALDINI ARRIGO s.r.l. con sede legale in Faenza (RA) – via Granarolo n.113 - codice fiscale 90035110395 – PI 02560670396 (per veicoli oggetto di sequestro)

2) ZINI ELIO Srl, con sede legale a Bologna in via Guido Reni n. 2/2 Partita Iva e C.F. 01543211203 (per veicoli in stato di abbandono)

3) AUTOCARROZZERIA GIAMPAOLO S.r.l., con sede in Castenaso (BO), Via Frullo n. 32, C.F. 03093840373 (per il servizio di interventi urgenti di spostamento di veicoli al fine di ripristinare le condizioni di sicurezza e di viabilità nel territorio comunale (es. divieti di sosta per lavori stradali, pulizia strade, feste ecc.)

- **SOCIETA' CHE PROVVEDE ALLA GESTIONE DELLA RISCOSSIONE, COATTA ED ORDINARIA, DELLE SANZIONI AMMINISTRATIVE:**

MAGGIOLI SPA con sede a Sant'Arcangelo di Romagna, Via del Carpino, 8 Cod. Fiscale 06188330150 e P. Iva 02066400405,

7. In caso di designazione di responsabili esterni del trattamento, il rapporto è stato debitamente contrattualizzato?

SI', mediante atto di nomina formale sottoscritto dalle parti ai sensi dell'art. 28 GDPR.

Per i Responsabili esterni al trattamento dati (software house) si veda l'allegato B

8. Trattamento automatizzato/manuale

Il trattamento è manuale attraverso ausilio degli strumenti elettronici e senza l'ausilio di strumenti elettronici. Tuttavia esiste un procedimento di trattamento automatizzato senza profilazione per quel che attiene i dati degli utenti che visitano il portale della Comune nel web.

9. Modalità di conservazione dei dati su supporto cartaceo o fisico

La conservazione dei dati su supporto cartaceo avviene all'interno di archivi predisposti a questo scopo e tutti presidiati da chiavi in possesso solo di soggetti designati e apicali.

La distruzione del documento avviene con tritadocumenti che riducono a strisce il documento da distruggere.

10. Modalità di conservazione dei dati su supporto informatizzato

Le dotazioni tecnologiche in uso presso il Comune di Castenaso sono:

SERVER	POSTAZIONI CLIENTS	DISPOSITIVI SMARTPHONE	STAMPANTI	FAX	DISPOSITIVI DI MEMORIZZAZIONE ESTERNI (es. HDD, SDD, USB drive)	WI-FI
N. 70 PRESSO D.P.O LEPIDA	**NUMERO TOTALE** - 143	N. 37 S.O. Android	N. 46	N. 2	N. 7	RETE DELLA P.A. DENOMINATA CASTORO accessibile solo mediante password assegnata a ogni dipendente o soggetto autorizzato; modificata ogni 3 mesi con rilascio telematico via email.

SERVER	POSTAZIONI CLIENTS	DISPOSITIVI SMARTPHONE	STAMPANTI	FAX	DISPOSITIVI DI MEMORIZZAZIONE ESTERNI (es. HDD, SDD, USB drive)	WI-FI
	PC FISSI: N. 101					RETE REGIONE E.R. ESTERNA OSPITI DENOMINATA **E.R. WI-FI**
	NOTEBOOK/ LAPTOP N. 42					RETE DELLA P.A. DENOMINATA **CAS-TORO**
	TABLET N. 5					

Ulteriore dotazione tecnologica interna alla società è costituita da telefoni cellulari e sim intestate al Titolare (Comune di Castenaso):

Smartphones **personali** così suddivisi:

- N. 37 con indirizzo account mail della P.A. configurato, con S.O. Android
- N. 1 con indirizzo account mail della P.A. NON configurato, con S.O. Android

Il tracciamento del dipendente per verificare la presenza avviene mediante il BADGE

11. Descrizione delle misure di sicurezza adottate nel trattamento automatizzato (art. 32)

La rete del Titolare è strutturata con una linea internet con fibra ottica

Risulta disponibile una rete wifi interna protetta da password e una WiFi Ospiti esterna e liberamente accessibile senza richiesta di password (Emilia Romagna Wifi Private)

- WiFi del COMUNE DI CASTENASO - NOME CAS-TORO per accesso a LAN interna
- WiFi Ospiti per sola navigazione accesso libero alla rete regionale esterna denominata Emilia Romagna Wifi Private

Gli strumenti informatici vengono utilizzati per la gestione della quasi totalità dei dati della P.A.

Attraverso i suddetti sistemi sono trattati i dati personali di utenti, cittadini, fornitori, e dipendenti.

- N. 101 - S.O. Windows 10 pro - Windows 11 pro PC fisici
- N. 42 - S.O.Windows 10 pro - Windows 11 pro notebook
- N. 5 - S.O. Windows 10 pro - Windows 11 pro TABLET

Server presso la struttura

- N. 1 Windows Server 2012 presso Polizia Locale

Server presso terzi (Presso farm DATA CENTER LEPIDA RAVENNA)

- N. 38 Windows Server 2012
- N. 28 Altri S.O. Diversi da Windows

MISURE DI SICUREZZA CON CREDENZIALI DI ACCESSO:

- Utente di dominio e password
- Su software in cloud MFA in fase di attivazione
- Per connessioni in modalità smart working MFA in fase di attivazione

MISURE DI AUTORIZZAZIONE AL SISTEMA INFORMATIVO AZIENDALE:

- Files System On-Premise: ogni utente possiede permessi propri a livello di filesystem e/o condivisione
- Applicativi in Cloud: ogni utente possiede permessi propri gestiti direttamente dal sistema Cloud

SOFTWARE APPLICATIVI IMPIEGATI NELLA P.A.:

- SUITE PROTOCOLLO E ATTI - ADS
- ANAGRAFE TRIBUTARIA CONTRATTI - AGENZIA DELLE ENTRATE
- ARCADIA – MAGGIOLI
- BOV BOLLO VIRTUALE – AGENZIA DELLE ENTRATE
- CARTELLINO E GIUSTIFICATIVI – ELCO SISTEMI
- CEDOLINO – ELCO SISTEMI
- CESSIONE FABBRICATI – DE AGOSTINI
- SUITE CF CONTABILITA‘ FINANZIARIA – ADS

- SUITE CG CONTROLLO DI GESTIONE E OBJ – ADS
- CIMITERO WEB – GRUPPO MARCHE
- CONCILIA – MAGGIOLI
- CONSULTA FABBRICATI – MICROSOFT ACCESS
- SUITE DATAGRAPH – DATAGRAPH
- DOCFA40 -
- ENTRATEL DESKTOP TELEMATICO – AGENZIA DELLE ENTRATE
- GRADUS – SOFTECH
- UNIEMENS – INPS
- BABYLON – GIES
- IRIDE – MAGGIOLI
- ISI-ISTATEL – MINISTERIALE
- JCONS – ADS
- MCTC EMULATORE – MCTC
- MUD – MINISTERIALE
- PAYROLL – MAGGIOLI
- PRYMUS – ACCA SOFTWARE

- SUAPNET – AMBITO
- SUITE CITYWARE – PALITALSOFT
- UNIMOD – AGENZIA DELLE ENTRATE

SOFTWARE APPLICATIVI CONTROLLO DA REMOTO

Software controllo remoto: Supremo - Logmein - Citrix - Ultra VNC

FIREWALL A PRESIDIO DEL SISTEMA INFORMATIVO:

- Zyxell Fornito da SEIT
- Firewall Wawey As A Service presso infrastruttura Datacenter Lepida
- Sophos FW XGS2100

ANTIVIRUS

Antivirus Sophos EndPoint Protection

LA P.A. E' DOTATA DI GRUPPO DI CONTINUITA' CHE GARANTISCE DURATA PER 4 ORE CONSECUTIVE

Descrizione del Sistema di Backup, Disaster Recovery e Contingency Planning:

Il backup della struttura di COMUNE DI CASTENASO avviene nella seguente modalità

- Copia primaria (snapshot e FileSystem) su spazio disco dedicato all'interno del Datacenter di Lepida sito in Ravenna
    - Full settimanale e incrementale giornaliero con retention di 14 giorni
- Copia secondaria su cloud esterno a Lepida

In caso di problemi software il **disaster recovery** è possibile. In caso di problemi fisici non esistono copie di backup esterne al sito dell'azienda. In caso di problemi software alle macchine il ripristino è possibile tra i 15 minuti e le 2 ore.

In caso di problemi hardware ai server fisici va aggiunto il tempo necessario al recupero di un nuovo server compatibile e il tempo necessario al ripristino di tutta la struttura.

Esiste un gruppo continuità che agisce e mantiene attive le macchine, 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, il Titolare del trattamento e il responsabile del trattamento hanno messo in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza appropriato al rischio, che comprendono:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento attraverso il sistema di backup;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico secondo il programma di contingency planning o ripristino dei dati;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

La notifica predeterminata in caso di violazione o perdita dei dati indica: la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione, nonché la comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni, nonché le probabili conseguenze della violazione dei dati personali;

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

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.

12. Liceità e finalità del trattamento (capo II)

I trattamenti effettuati sono compiuti per poter adempiere agli obblighi istituzionali e contrattuali che il Titolare ha assunto nei confronti degli interessati/dipendenti e cittadini, cui i dati appartengono, in ragione e nel rispetto del contratto di lavoro subordinato e delle norme in materia di diritto del lavoro, degli interessati/ o collaboratori in ragione e nel rispetto del contratto sottoscritto dalle parti e dalle norme in materia. I dati dei cittadini/utenti invece, sono trattati in adempimento agli obblighi di legge ed istituzionali e all'interesse legittimo assunte verso gli stessi, o previa autorizzazione concessa dai cittadini/utenti stessi, a conseguire dati e recapiti personali (email personale o personificata) allo scopo di inviare informazioni di tipo diverso da quello istituzionale.

13. E' disponibile un elenco degli interessati coinvolti nel trattamento?

Sì, sono i dipendenti e tutti i cittadini residenti presso il Comune di Castenaso costituenti l'utenza del territorio.

14. Tabella analitica dei dati coinvolti nel trattamento

DATI ANAGRAFICI CITTADINO, UTENTE, DIPENDENTE, COLLABORATORE, CARICA ISTITUZIONALE	DATI FISCALI CITTADINO, COLLABORATORE, DIPENDENTE, CARICA ISTITUZIONALE	DATI PARTICOLARI DEL DIPENDENTE O CITTADINO O UTENTE	DATI BANCARI FINANZIARI CITTADINO (SE OCCORRE E PER FINI DI IMPOSTA) - DIPENDENTE O CARICA ISTITUZIONALE	DATI INFORMATICI CITTADINO, DIPENDENTE O COLLABORATORE, CARICA ISTITUZIONALE
nome e cognome	C.F.	DATI DELLA SALUTE: malattie, infortuni, inabilità, invalidità, dati per la	codice iban	

DATI ANAGRAFICI CITTADINO, UTENTE, DIPENDENTE, COLLABORATORE, CARICA ISTITUZIONALE	DATI FISCALI CITTADINO, COLLABORATORE, DIPENDENTE, CARICA ISTITUZIONALE	DATI PARTICOLARI DEL DIPENDENTE O CITTADINO O UTENTE	DATI BANCARI FINANZIARI CITTADINO (SE OCCORRE E PER FINI DI IMPOSTA) - DIPENDENTE O CARICA ISTITUZIONALE	DATI INFORMATICI CITTADINO, DIPENDENTE O COLLABORATORE, CARICA ISTITUZIONALE
		prevenzione salute pubblica		
recapito terrestre o recapito digitale,	PIVA	DATI POLITICI: iscrizione sindacato, o destinazione dell'8 per mille a partito o sindacato	conto corrente bancario	indirizzo IP
recapito email e recapito		DATI IDEOLOGICI:	reddito	

DATI ANAGRAFICI CITTADINO, UTENTE, DIPENDENTE, COLLABORATORE, CARICA ISTITUZIONALE	DATI FISCALI CITTADINO, COLLABORATORE, DIPENDENTE, CARICA ISTITUZIONALE	DATI PARTICOLARI DEL DIPENDENTE O CITTADINO O UTENTE	DATI BANCARI FINANZIARI CITTADINO (SE OCCORRE E PER FINI DI IMPOSTA) - DIPENDENTE O CARICA ISTITUZIONALE	DATI INFORMATICI CITTADINO, DIPENDENTE O COLLABORATORE, CARICA ISTITUZIONALE
telefonico fisso o mobile		iscrizione e destinazione 8 per mille a associazioni		
data e luogo di nascita		DATI RELIGIOSI: iscrizione e destinazione per 8 per 1000 a chiesa cattolica o altra fede religiosa		

DATI ANAGRAFICI CITTADINO, UTENTE, DIPENDENTE, COLLABORATORE, CARICA ISTITUZIONALE	DATI FISCALI CITTADINO, COLLABORATORE, DIPENDENTE, CARICA ISTITUZIONALE	DATI PARTICOLARI DEL DIPENDENTE O CITTADINO O UTENTE	DATI BANCARI FINANZIARI CITTADINO (SE OCCORRE E PER FINI DI IMPOSTA) - DIPENDENTE O CARICA ISTITUZIONALE	DATI INFORMATICI CITTADINO, DIPENDENTE O COLLABORATORE, CARICA ISTITUZIONALE
luogo di residenza		DATI GIUDIZIARI: condanne penali del casellario giudiziale del dipendente o del cittadino		

15. Modalità di resa dell'informativa agli interessati

L'informativa è fornita su supporto esclusivamente digitale pubblicato per dipendenti e cittadini sul sito del Comune al seguente link: https://www.comune.castenaso.bo.it/it-it/amministrazione/amministrazione-trasparente/altri-contenuti/dati-ulteriori/privacy

Tuttavia esiste come alternativa l'informativa cartacea che è reperibile dietro richiesta espressa alla P.A., laddove non si abbia modo di poterla stampare o visualizzare. Tale modalità è da ritenersi residuale e solo dietro espressa richiesta motivata.

La forma cartacea è in ogni caso affissa presso gli sportelli e gli uffici accessibili al pubblico per consentirne comunque l'accessibilità a chiunque intenda consultarla e conoscerne il contenuto.

16. Modalità di raccolta del consenso, se richiesto quale base giuridica, rettifica e cancellazione da parte degli interessati

La modalità prevista è in modo diretto, per iscritto o in alternativa raccolta mediante la registrazione del consenso on line, espresso con un flag, negli apposti spazi nel sito istituzionale e registrato nel server della p.a.

17. Eventuale presenza di processi automatizzati limitazioni (Capo III sezione 4 e 5)

Non ci sono.

18. Esiste una procedura per la gestione di una richiesta di portabilità dei dati? (art. 20)

Sì. Il diritto alla portabilità riguarda anche i dati forniti attraverso la fruizione di un servizio o l'utilizzo di un dispositivo, come la *cronologia delle ricerche,* le informazioni che riguardano il *traffico*, i dati relativi all'*ubicazione*. Il diritto alla portabilità dei dati può essere esercitato quando:

1 i dati personali (anche particolari) siano trattati sulla base del consenso preventivo dell'interessato oppure in esecuzione di un contratto di cui l'interessato è parte, o ancora di misure precontrattuali adottate su sua richiesta.

2 che il trattamento sia effettuato con mezzi automatizzati. Saranno esclusi quindi i dati conservati in archivi ed elenchi cartacei.

Gli unici dati automatizzati confortati da consenso e oggetto di potabilità sono i dati raccolti dalla videosorveglianza e dai cookies analytics.

19. Modalità di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (art. 25)

E' stato analizzato l'intero modo di trattare i dati ponendo l'utente al centro, mirando ad una tutela effettiva da un punto sostanziale, non solo formale, cioè non è sufficiente che la progettazione dei sistema sia conforme alla norma se poi l'utente non è tutelato.

L'obbligo di *privacy by design* è basato sulla valutazione del rischio. Tale valutazione è stata fatta al momento della progettazione del sistema, quindi prima che il trattamento inizi. Chiaramente abbiamo tenuto conto anche del tipo di dati trattati, per cui in presenza di un trattamento che coinvolge dati sensibili, gli obblighi dovranno essere più stringenti, in considerazione del fatto che il rischio è maggiore.

L'approccio basato sul rischio comporta che si deve tenere conto dello stato della tecnologia, per cui il trattamento va adattato nel corso del tempo.

La P.A. ha sposato un approccio *risk based* avente l'evidente vantaggio di pretendere degli obblighi che possono andare oltre la mera conformità alla legge, sicuramente più flessibile e adattabile al mutare delle esigenze e degli strumenti tecnologici, ma anche valutando il rischio, rendendo quindi più difficili le contestazioni in caso di violazioni.

Nel rispetto del principio di *privacy by default*, per impostazione predefinita l'Ente tratta solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini.

L'Ente ha stabilito nel proprio modello organizzativo di predisporre una valutazione di impatto privacy ogni volta che implementa un nuovo procedimento che prevede un trattamento di dati.

20. Modalità di consultazione preventiva, se applicabile (art. 36)

Non è applicabile per la tipologia di trattamenti effettuati e di dati trattati.

21. Valutazione di impatto sulla protezione dei dati se appropriata (art. 35)

In relazione al Regolamento 2016/679, è stata effettuata una verifica di conformità, come parte di DPIA, secondo quanto illustrato nella appendice B a questo documento e siamo giunti alla seguente conclusione:

il trattamento dei dati personali avviene con adeguati mezzi di tutela organizzativa e tecnica

22. procedure di gestione di una violazione dei dati (artt. 33 e 34)

Per fronteggiare le ipotesi in cui i dati siano colpiti da eventi che possano danneggiarli, o addirittura distruggerli, vengono previsti criteri e modalità tali, da garantire il loro ripristino in termini ragionevoli, e comunque entro una settimana per tutti i tipi di dati elettronici.

I dati personali conservati, trasmessi o trattati da aziende e pubbliche amministrazioni possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità. Si tratta di situazioni che possono comportare pericoli significativi per la privacy degli interessati cui si riferiscono i dati.

Per questa ragione, anche sulla base della normativa europea, il Garante per la protezione dei dati personali ha adottato negli ultimi anni una serie di provvedimenti che introducono l'obbligo di comunicare eventuali violazioni di dati personali (data breach) all'Autorità stessa e, in alcuni casi, anche ai soggetti interessati. Il mancato o ritardato adempimento della comunicazione espone alla possibilità di sanzioni amministrative.

Il regolamento europeo, nell’ottica di venire incontro alle esigenze delle pubbliche amministrazioni e delle aziende e evitare un enorme danno reputazionale, specifica che non è richiesta la comunicazione all'interessato se è soddisfatta almeno una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

La data breach mette al centro dell'organizzazione la valutazione del rischio; occorre infatti, valutare la particolare probabilità e gravità del rischio, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio; occorre valutare anche il rischio per i cittadini e gli utenti e verificare se è elevato (ad esempio quando si tratti di frode, furto di identità, danno all'immagine etc.).

Il Regolamento, per gli altri profili, distingue due ipotesi:

1. Il primo caso è disciplinato dall'art.33 GDPR, che impone di notificare la violazione dei dati personali all'Autorità di controllo nazionale competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Nel caso in cui non venga effettuata la notifica entro 72 ore, è ancora possibile farla, ma deve essere corredata dai motivi del ritardo.

La norma prevede anche il contenuto minimo che la comunicazione all'Autorità Garante dovrà avere:

"a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.".

2. Il Regolamento impone la comunicazione al Garante, ma anche la comunicazione della violazione dei dati personali “data breach” verso il soggetto interessato (cittadino, utente), comunicazione che è richiesta, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Il legislatore comunitario, a tale proposito, ritiene che se l’interessato (cittadino o utente) è avvertito della violazione può prendere le precauzioni necessarie in materia. La sopra citata comunicazione deve essere effettuata dal titolare senza ingiustificato ritardo.

Il regolamento richiede che la comunicazione all'interessato (cittadino) deve essere effettuata, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere allo stesso la natura della violazione dei dati personali verificatesi.

Il regolamento specifica il contenuto minimo (le informazioni e le misure) con un richiamo al sopra citato art. 33, paragrafo 3, lettere b), c) e d) del regolamento che ricompense la comunicazione dovuta.

COME PREPARARE LA COMUNICAZIONE

1 la comunicazione dei riferimenti e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni (lett.b);

2 la descrizione delle probabili conseguenze della violazione dei dati personali (lett.c);

3 la descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi (lett.d).

In caso di *Data Breach* il Responsabile, di concerto con il Titolare, deve procedere a verificare anche la causa e l'origine del sinistro telematico, la sussistenza di perdita di dati o compromissione del sistema informativo aziendale.

Secondo questo *contingency planning*, il *disaster recovery* prevede il ripristino dei dati che sono periodicamente salvati mediante il *backup*.

Per i dati trattati con strumenti elettronici, sono previste procedure di backup, attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema, su dispositivi informatici.

23. Luoghi di trattamento dei dati

Sede principale del Titolare e presso la ubicazione dei data center eletti su cui sono allocati i dati.

24. Luoghi di conservazione dei dati

Le copie vengono custodite in luoghi protetti della sede, ad accesso controllato.

25.Durata di conservazione dei dati, con giustificazione di tale durata e modalità di cancellazione (artt. 17 e 19)

TEMPO CONSERVAZIONE DATI CONTABILI	TEMPI DI CONSERVAZIONE DATI PERSONALI ANAGRAFICI	TEMPI DI CONSERVAZIONE DATI BANCARI - DATI FINANZIARI	TEMPI DI CONSERVAZIONE DATI PARTICOLARI	TEMPI DI CONSERVAZIONE TRAFFICO TELEMATICO
10 ANNI	10 ANNI DOPO LA CONCLUSIONE DEL RAPPORTO O A RICHIESTA DELLL'INTERESSATO	10 ANNI DOPO LA CONCLUSIONE DEL RAPPORTO O A RICHIESTA DELLL'INTERESSATO	10 ANNI DOPO LA CONCLUSIONE DEL RAPPORTO O A RICHIESTA DELLL'INTERESSATO SE NON VI E' OBBLIGO DI LEGGE	6 MESI O A RICHIESTA DELL'INTERESSATO

26. Modalità particolari di trattamento se applicabili (capo IX)

Non applicabili.

27. Elenco dei titolari del trattamento, terzi, domiciliati nell'Unione Europea, cui i dati vengono comunicati

- I.N.P.S.
- I.N.A.I.L.
- ISTITUTI BANCARI USATI DALLA P.A.
- GESTORE TELEFONICO E TELEMATICO
- INTERNET HOSTING PROVIDER
- TERZI ESTERNI CON CUI HA RAPPORTI LA P.A. PER RAGIONI ISTITUZIONALI E DI FUNZIONE

28. Trasferimento dei dati all’esterno della UE e descrizione delle modalità di trasferimento (capo V)

Non avviene.

29. Trattamento conforme ai codici di condotta (art. 40)

Il Titolare non ha ancora aderito ad alcun codice di condotta.

30. In caso coordinate dell’azienda che svolge l’attività di monitoraggio (art. 41)

Non esiste.

31. Trattamento conforme a certificazioni o sigilli europei (art. 42)

Non sono state conseguite.

32. Coordinate e qualifiche del responsabile della protezione dei dati se designato (art. 37)

Il Responsabile per la protezione dei dati personali (Data Protection Officer - “DPO”) del Comune di Castenaso è stato regolarmente designato e formalmente incaricato, pertanto risulta raggiungibile fino al 31.12.2023 al seguente indirizzo e-mail: dpo-team@lepida.it

A far data dal 01.01.2024 il nuovo DPO, Avv. Chiara Ciccia Romito, sarà raggiungibile al seguente indirizzo e-mail: dpo.comune.castenaso@lawfirmstudio.it

33. In caso di designazione di un responsabile esterno della protezione dei dati, il rapporto è stato debitamente contrattualizzato?

Si

34. Se l’organizzazione gestisce un sito web è stata definita una politica di protezione dei dati (privacy policy) ed essa è chiaramente visualizzata sulla home page del sito?

Si

34. Tale politica minimizza la acquisizione e gestione di eventuali marcatori (cookies)?

Si

36. E’ stato designato un web master responsabile per il rispetto della privacy policy e del costante aggiornamento delle misure di sicurezza anti- intrusione ed anti- infezione del sito web?

Si

37. Eventuali altre informazioni afferenti al trattamento dei dati

_____-