Guida di Korevium Privacy

Indice

1. 1. Benvenuto
2. 2. Installazione e primo avvio
3. 3. Attivare la licenza
4. 4. Come è fatta la finestra
5. 5. Elenchi e maschere: come si usano
6. 6. Esempio completo: un ristorante dall'inizio alla fine
7. 7. Titolari del trattamento
8. 8. Registro dei trattamenti
9. 9. Analisi dei rischi
10. 10. Soggetti e nomine
11. 11. Informative
12. 12. Valutazione d'impatto (DPIA)
13. 13. Registro violazioni (data breach)
14. 14. Richieste degli interessati
15. 15. Formazione del personale
16. 16. Scadenzario
17. 17. Riepilogo conformità
18. 18. Questionario e copia dei trattamenti
19. 19. Procedure rapide
20. 20. Pacchetto normativo
21. 21. Assistente Korevium Privacy
22. 22. Database e uso in rete
23. 23. Backup e ripristino
24. 24. Sync cloud
25. 25. Licenza e versione dimostrativa
26. 26. Aggiornamenti
27. 27. Assistenza
28. 28. La disciplina: le fonti e come leggerle
29. 29. La disciplina: principi e responsabilizzazione
30. 30. La disciplina: i ruoli
31. 31. La disciplina: il doppio ruolo degli studi professionali
32. 32. La disciplina: basi giuridiche e categorie particolari
33. 33. La disciplina: informative e trasparenza
34. 34. La disciplina: i diritti degli interessati
35. 35. La disciplina: sicurezza e analisi dei rischi
36. 36. La disciplina: valutazione d'impatto (DPIA) e consultazione preventiva
37. 37. La disciplina: violazioni dei dati (data breach)
38. 38. La disciplina: conservazione dei dati
39. 39. La disciplina: lavoratori, videosorveglianza e geolocalizzazione
40. 40. La disciplina: trasferimenti fuori dall'Unione europea
41. 41. La disciplina: sanzioni e responsabilità
42. 42. La disciplina: tenere tutto in ordine nel tempo
43. 43. Obblighi GDPR e dove si gestiscono
44. 44. Glossario

1. Benvenuto

Korevium Privacy è il programma per tenere in ordine gli adempimenti privacy di uno o più **titolari del trattamento** (aziende, studi professionali, professionisti, associazioni, enti) secondo il Regolamento (UE) 2016/679 (GDPR) e il D.Lgs. 196/2003 (Codice privacy): registro dei trattamenti, nomine, informative, valutazioni d'impatto, violazioni dei dati, richieste degli interessati, formazione e scadenze.

Nel programma il soggetto per cui si tengono gli adempimenti si chiama **titolare del trattamento**: è il termine del GDPR (art. 4, n. 7) e indica chi decide perché e come si trattano i dati. Può essere un'impresa, uno studio, un professionista o un ente.

A chi serve

- all'**impresa, allo studio o al professionista** che gestisce da sé la propria privacy (edizione Mono);
- al **consulente, commercialista o DPO** che segue la privacy di più titolari, ad esempio i propri clienti (edizione Multi).

I dati restano tuoi: il programma lavora sul tuo PC (o sul disco di rete dell'ufficio) e non invia nulla su internet. Se vuoi lavorare da più PC in luoghi diversi puoi usare Sync cloud con la tua cartella di Google Drive o OneDrive.

Come usare questa guida: a sinistra c'è l'indice, in alto la casella per cercare una parola (ad esempio «nomina» o «72 ore»). Il pulsante **Esporta guida in PDF** crea il manuale completo da stampare. La guida si apre da qualsiasi punto con il tasto **F1**.

Da dove cominciare: se è la prima volta leggi i capitoli 2 «Installazione e primo avvio», 4 «Come è fatta la finestra» e 6 «Esempio completo»; poi consulta i capitoli delle singole pagine quando ti servono. La seconda parte della guida, **«La disciplina»**, spiega le regole del GDPR e del Codice privacy che stanno dietro a ogni pagina.

Hai un dubbio? Oltre a questa guida c'è l'**Assistente Korevium Privacy**: pulsante **Assistente** in alto, oppure Sistema › Assistente Korevium Privacy. Apre sul sito una chat che risponde sull'uso del programma e sugli adempimenti.

2. Installazione e primo avvio

Installazione: esegui il programma di installazione ricevuto (oppure apri **Korevium Privacy.exe** nella cartella del programma). Sul desktop e nel menu Start compare l'icona Korevium: la K nell'esagono dorato.

Primo avvio

1. Compare la **schermata di avvio** con il nome del programma e la versione.
2. Compare il **Contratto di licenza d'uso**: leggilo, metti la spunta «Ho letto e accetto…» e premi **Accetto**. Se premi **Non accetto** il programma si chiude. Il contratto viene richiesto di nuovo solo quando cambia.
3. Il programma si apre in **versione dimostrativa** (barra rossa in alto): puoi provarlo con 1 titolare e 5 trattamenti. Per usarlo senza limiti attiva la licenza (capitolo «Licenza e versione dimostrativa»).

Dove vengono salvati i dati: nel file **privacy.db** nella cartella *%APPDATA%\Korevium\Privacy* (per aprirla: Sistema › Apri cartella dei dati). Puoi spostarli su un disco di rete o NAS da Sistema › Cartella del database.

Disinstallazione: disinstallando il programma i dati restano nella cartella dei dati; per conservarli altrove fai prima un backup (Sistema › Backup e ripristino).

3. Attivare la licenza

1. Premi il pulsante bianco sotto «Esci dal programma» (oppure **Sistema › Licenza**).
2. Se non hai ancora il codice premi **Richiedi la licenza…**: si apre un'email già preparata per l'assistenza; completa intestatario, partita IVA e dati per la fattura e inviala.
3. Quando ricevi il **codice di attivazione**, copialo (Ctrl+C) e incollalo (Ctrl+V) nella casella grande, oppure premi **Carica da file…** se lo hai ricevuto come file .key.
4. Premi **Attiva**: compare «Licenza attivata». Chiudi e riapri il programma.

Al riavvio la barra rossa scompare e a sinistra leggi l'edizione e la data di scadenza.

Su più PC: la licenza è intestata alla partita IVA e vale su tutti i PC dell'intestatario. Su ogni PC ripeti i punti 1, 3 e 4 con lo stesso codice.

Rinnovo: un mese prima della scadenza il pulsante a sinistra lo segnala. Premi **Richiedi rinnovo…** e, ricevuto il nuovo codice, attivalo nello stesso modo.

4. Come è fatta la finestra

Barra laterale (a sinistra)

- nome del programma e pulsante **Esci dal programma**;
- pulsante bianco con lo **stato della licenza**: cliccandolo si apre la finestra Licenza;
- **Aree di gestione**: le pagine del programma (Registro dei trattamenti, Soggetti e nomine, DPIA, Registro violazioni, Richieste degli interessati, Formazione, Scadenzario, Riepilogo conformità, Titolari del trattamento, Sistema);
- **Documenti / Stampa**: comandi rapidi (stampa del registro, informativa, questionario per il cliente, copia dei trattamenti, aggiorna dati).

Barra superiore: le stesse aree in forma di icone (passando il mouse compare il nome), la casella **Titolare** per scegliere il titolare del trattamento su cui lavorare e i pulsanti **Assistente** e **Aggiornamenti**.

Area centrale: il titolo della pagina, una riga di spiegazione e il riquadro blu **Titolare del trattamento** con nome, partita IVA e comune del titolare scelto. Tutto ciò che inserisci riguarda quel titolare.

Piè di pagina: lo stato («Pronto» oppure «Sola lettura») e la versione del programma.

Barra rossa: compare solo per segnalare la versione dimostrativa, la licenza in scadenza o scaduta, oppure il database aperto in sola lettura.

5. Elenchi e maschere: come si usano

Gli elenchi: ogni pagina mostra un elenco con, sopra, la barra dei pulsanti.

- **Cerca**: scrivi una parola e l'elenco mostra solo le righe che la contengono.
- **Nuovo**: apre la maschera vuota. **Modifica** (oppure doppio clic sulla riga): apre la riga selezionata.
- **Duplica**: crea una copia della riga selezionata, utile per trattamenti simili.
- **Elimina**: cancella la riga dopo una conferma. Eliminando un titolare si cancellano anche tutti i suoi dati.
- 📎 **Allegati**: collega file alla riga (contratti firmati, attestati, verbali). Si aprono con doppio clic.
- **Stampa PDF** ed **Esporta Excel**: stampano o esportano le righe visibili.

Cliccando sull'intestazione di una colonna l'elenco si ordina. I **colori delle righe** segnalano qualcosa da guardare: rosso = scaduto o rischio alto, arancione = in scadenza, grigio = cessato.

Le maschere: sono divise in schede (in alto). In basso c'è il riquadro giallo degli **avvisi**, che il programma aggiorna mentre scrivi (ad esempio quando serve la DPIA).

- I campi con ***** sono obbligatori; quelli con ⓘ mostrano un suggerimento passandoci sopra con il mouse.
- **Date**: scrivi gg/mm/aaaa, oppure usa il calendario 🗓️ o il pulsante **Oggi**.
- **Caselle di spunta**: spunta tutte le voci che servono. Nella riga **Altro** puoi aggiungere voci non presenti, separate da punto e virgola (es. «Clienti esteri; Agenti»).
- **Tendine**: scegli una voce dall'elenco; in molte puoi anche scrivere un testo libero.
- I campi grigi in grassetto sono **calcolati dal programma** (rischio, termini, scadenze).

Premi **Salva** per registrare, **Annulla** per uscire senza salvare.

6. Esempio completo: un ristorante dall'inizio alla fine

Questo esempio mostra il percorso tipico per mettere in regola un titolare del trattamento. I dati sono inventati.

1. **Titolare** — Titolari del trattamento › Nuovo: «Prova Ristorante Srl», P.IVA 01234567890, Via Roma 1, 84091 Battipaglia (SA), legale rappresentante Mario Rossi. Scheda Privacy: DPO nominato «No», data aggiornamento: Oggi. Salva.

2. **Raccolta informazioni** — Documenti / Stampa › Questionario per il cliente: lo mandi al ristorante e lo usi come traccia per i passaggi successivi.
3. **Trattamenti** — Registro dei trattamenti › Da modello…: «Gestione del personale dipendente», «Gestione amministrativo-contabile dei clienti», «Gestione dei fornitori», «Videosorveglianza». Apri ciascuno e adatta finalità, dati e misure alla realtà del ristorante.
4. **Fornitori e personale** — Soggetti e nomine › Nuovo: «Studio Paghe Bianchi» come Responsabile del trattamento (art. 28), attività «elaborazione buste paga»; «Anna Verdi» come Autorizzato al trattamento (art. 29), con il trattamento «Gestione del personale dipendente». Torna nei trattamenti e, nella scheda Destinatari, spunta Studio Paghe Bianchi tra i responsabili esterni.
5. **Analisi dei rischi** — in ogni trattamento compila la scheda Analisi dei rischi. Sulla videosorveglianza il programma avvisa che, con due criteri di rischio, la DPIA è di norma necessaria.
6. **DPIA** — Valutazioni d'impatto › Nuova da trattamento… › Videosorveglianza: completa le sezioni e premi **DPIA in Word**.
7. **Documenti** — Soggetti e nomine › Genera nomina (Word) per ogni soggetto; Informativa (Word) per Dipendenti e per Clienti. Fai firmare le nomine, inserisci la data nomina e allega il documento firmato con 📎 Allegati.
8. **Formazione** — registra il corso fatto al personale, con il prossimo aggiornamento tra un anno.
9. **Controllo** — Riepilogo conformità: guarda la percentuale e l'elenco dei requisiti non soddisfatti, sistema quelli che mancano. Stampa il registro in PDF e consegnalo al cliente insieme alla verifica di conformità.
10. **Nel tempo** — lo Scadenzario ti ricorda revisioni, nomine in scadenza e formazione. Se succede una violazione la registri nel Registro violazioni; se un cliente chiede i suoi dati, in Richieste degli interessati.

7. Titolari del trattamento

Ogni titolare del trattamento (impresa, studio, professionista, associazione, ente) ha il proprio registro, i propri soggetti e i propri registri di violazioni, richieste e formazione. Il numero di titolari dipende dall'edizione della licenza: con l'edizione Mono si gestisce solo il titolare intestatario della licenza (stessa partita IVA o codice fiscale), con l'edizione Multi tutti quelli che servono.

Uno **studio professionale** che segue la privacy dei clienti inserisce sé stesso (per i propri trattamenti: dipendenti, clienti dello studio, fornitori) e ciascun cliente come titolare distinto. Quando lo studio tratta dati per conto di un cliente, quei trattamenti vanno nel **registro del responsabile** dello studio (capitolo «La disciplina: il doppio ruolo degli studi»).

Scheda Dati del titolare

Campo	Cosa scrivere
Ragione sociale / Nome *	Denominazione completa, come in visura (es. «Prova Ristorante Srl»).
Forma giuridica	Scegli dall'elenco (Srl, Srls, ditta individuale, libero professionista…).
Partita IVA / Codice fiscale	Compaiono nel registro, nelle nomine e nelle informative.
Indirizzo, CAP, Comune, Provincia	Sede legale. Il comune viene usato anche come luogo nelle firme.
PEC, Email, Telefono, Sito web	Contatti del titolare: finiscono nelle informative come recapiti per gli interessati.
Legale rappresentante	Chi firma i documenti come titolare del trattamento.

Scheda Privacy

Campo	Cosa scrivere

Referente interno privacy	La persona del titolare che si occupa della privacy (non è un obbligo di legge, ma è utile indicarla).
DPO nominato / nome / contatti	Solo se il titolare ha designato un Responsabile della protezione dei dati. I contatti compaiono nelle informative.
Rappresentante nell'UE	Solo per titolari con sede fuori dall'Unione europea (art. 27).
Data ultimo aggiornamento del registro	Aggiornala ogni volta che rivedi il registro: serve allo scadenzario (revisione periodica) e al riepilogo di conformità.
Note	Annotazioni libere.

8. Registro dei trattamenti

Ogni riga è un'**attività di trattamento**: un insieme di operazioni sui dati con la stessa finalità (es. «gestione del personale», «videosorveglianza»). Il registro è previsto dall'art. 30 GDPR.

Da modello… crea un trattamento già compilato da uno dei sette modelli; poi va sempre adattato. **Scheda PDF** stampa il trattamento selezionato; **Stampa registro PDF** stampa il registro completo del titolare, diviso tra registro del titolare e registro del responsabile, con l'elenco dei soggetti. Se ci sono trattamenti cessati il programma chiede se includerli.

Scheda Generale

Campo	Cosa scrivere
Registro *	«Titolare (art. 30.1)» per i trattamenti che il titolare fa per sé; «Responsabile (art. 30.2)» per quelli che fa per conto di clienti (es. lo studio paghe che elabora i cedolini dei clienti).
Codice	Numerazione interna libera (T01, T02…): aiuta a citare i trattamenti nei documenti.
Denominazione *	Nome breve e chiaro (es. «Gestione del personale dipendente»).
Titolare per conto del quale si tratta	Solo per il registro del responsabile: nome e contatti del cliente titolare.
Contitolari	Spunta i soggetti con ruolo di contitolare (prima vanno inseriti in Soggetti e nomine).
Area / ufficio, Referente interno	Chi se ne occupa presso il titolare.
Stato	«Attivo» oppure «Cessato» (i cessati restano in archivio, in grigio).

Scheda Finalità

Campo	Cosa scrivere
Finalità *	Perché si trattano i dati, in modo concreto (es. «elaborazione delle retribuzioni, adempimenti contributivi e fiscali, gestione presenze»).
Base giuridica	Su cosa si fonda il trattamento (art. 6): contratto, obbligo di legge, consenso, legittimo interesse… Si possono spuntare più basi.
Descrizione del legittimo interesse	Obbligatoria nei fatti se hai scelto il legittimo interesse: spiega quale interesse (es. «tutela del patrimonio aziendale»).

Scheda Interessati e dati

Campo	Cosa scrivere

Categorie di interessati	Di chi sono i dati (dipendenti, clienti, fornitori, candidati, utenti del sito…). Le informative si generano proprio per queste categorie.
Categorie di dati personali	Quali dati (anagrafici, contatto, bancari, immagini…).
Categorie particolari (art. 9)	Dati sensibili: salute, sindacato, biometrici… Se ne spunti una, indica anche la condizione dell'art. 9.2 (il programma lo ricorda).
Condizione art. 9.2	La ragione che permette di trattare i dati particolari (es. obblighi in materia di lavoro).
Dati giudiziari (art. 10)	«Sì» se si trattano dati su condanne e reati (es. casellario).
Fonte dei dati	Se i dati arrivano dall'interessato o da terzi: cambia il contenuto dell'informativa (art. 14).

Scheda Destinatari

Campo	Cosa scrivere
Categorie di destinatari	A chi vengono comunicati i dati (consulente del lavoro, banche, enti previdenziali…).
Responsabili esterni (art. 28)	Spunta i fornitori inseriti in Soggetti e nomine che trattano questi dati: servono per le nomine e per i controlli di conformità.
Trasferimento verso paesi terzi	«Sì» se i dati vanno fuori dall'UE (es. servizi cloud americani).
Paesi terzi, Garanzie	Dove vanno i dati e su quale base (decisione di adeguatezza, Data Privacy Framework, clausole contrattuali standard…).

Scheda Conservazione e sicurezza

Campo	Cosa scrivere
Termine di conservazione	Per quanto tempo si tengono i dati (es. 10 anni per i documenti contabili, 72 ore per la videosorveglianza).
Criterio / note	Spiegazione del termine o casi particolari.
Modalità	Cartacea, informatica locale, cloud.
Strumenti e applicativi	Programmi e archivi usati (gestionale, software paghe, armadi…).
Misure tecniche e organizzative (art. 32)	Le protezioni adottate: password, backup, antivirus, armadi chiusi, formazione, istruzioni scritte…

Scheda Analisi dei rischi

Vedi il capitolo «Analisi dei rischi».

Scheda Valutazioni

Campo	Cosa scrivere
Informativa resa	«Sì» quando hai consegnato l'informativa agli interessati.
Consenso raccolto	«Non necessario» se la base non è il consenso; altrimenti «Sì» o «No».
Valutazione d'impatto (DPIA)	Non necessaria, Necessaria, Da valutare, Effettuata.

Data DPIA, Data inizio, Data ultima revisione	La data di revisione serve allo scadenzario: il trattamento va riguardato almeno una volta l'anno.

9. Analisi dei rischi

Nella scheda **Analisi dei rischi** di ogni trattamento si valuta quanto il trattamento può danneggiare le persone.

1. **Criteri di rischio presenti**: spunta quelli che ricorrono (monitoraggio sistematico, dati sensibili, larga scala, interessati vulnerabili come dipendenti o minori, nuove tecnologie…). Sono i criteri delle linee guida europee: **con due o più criteri la DPIA è di norma necessaria** e il programma lo segnala.
2. **Probabilità** che si verifichi un problema (accesso abusivo, perdita, errore) **prima** delle misure di sicurezza, da 1 Bassa a 4 Molto alta.
3. **Gravità** delle conseguenze per le persone, da 1 Trascurabile a 4 Massima.
4. Il programma calcola il **Rischio inerente** (probabilità × gravità): Basso, Medio, Alto, Molto alto.
5. **Principali minacce**: descrivi cosa può succedere (furto del PC, email sbagliata, attacco informatico…).
6. **Probabilità e gravità dopo le misure**: come cambiano grazie alle protezioni adottate. Il programma calcola il **Rischio residuo**.

Esempio: gestione del personale. Probabilità 2 (Media), gravità 3 (Significativa: ci sono dati sanitari) → rischio inerente Medio/Alto. Con password personali, backup e armadi chiusi la probabilità scende a 1 → rischio residuo Medio.

Le righe del registro con rischio residuo **Alto** o **Molto alto** sono rosse: valuta misure ulteriori o la DPIA.

10. Soggetti e nomine

Qui registri tutte le persone e le società coinvolte nei trattamenti.

I ruoli

Ruolo	Chi è	Documento generato
Responsabile del trattamento (art. 28)	Il fornitore che tratta dati per conto del titolare: consulente del lavoro, commercialista per le paghe, software house, hosting, assistenza informatica.	Atto di designazione del responsabile
Sub-responsabile (art. 28.4)	Il fornitore di cui si serve il responsabile.	Atto di designazione (sub-responsabile)
Contitolare (art. 26)	Un altro soggetto che decide insieme finalità e mezzi.	Accordo di contitolarità
Autorizzato (art. 29)	Dipendenti e collaboratori interni che trattano i dati.	Lettera di autorizzazione con istruzioni
Amministratore di sistema	Chi gestisce server, reti e PC (interno o esterno).	Designazione (Provvedimento del Garante 27/11/2008)
DPO	Il Responsabile della protezione dei dati, se nominato.	Atto di designazione del DPO

I campi

Campo	Cosa scrivere
Nome / Ragione sociale *, Ruolo *	Chi è e che ruolo ha.
Partita IVA / Codice fiscale, Indirizzo, Email / PEC	Finiscono nell'intestazione del documento di nomina.
Referente / firmatario	Chi firma per il soggetto (per le società).
Attività affidate / mansioni	Cosa fa: compare nel documento (es. «elaborazione buste paga»).
Trattamenti interessati	Per autorizzati e amministratori di sistema spunta i trattamenti a cui accedono. Per responsabili e contitolari il programma usa anche i trattamenti in cui li hai indicati.
Data nomina / contratto	Inseriscila dopo la firma: senza data il riepilogo segnala la nomina come mancante.
Scadenza nomina / contratto	Se c'è: lo scadenzario la ricorda e la riga diventa rossa quando è scaduta.
Tratta dati fuori dall'UE	Cambia una clausola dell'atto di designazione.

Procedura

1. Inserisci il soggetto e salva.
2. Selezionalo e premi **Genera nomina (Word)**: scegli dove salvarla, si apre in Word già compilata.
3. Rileggila, completala se serve e falla firmare.
4. Inserisci la **data nomina** e collega il documento firmato con **Allegati**.

11. Informative

L'informativa (artt. 13-14 GDPR) spiega agli interessati chi tratta i loro dati, perché, per quanto tempo e quali diritti hanno.

1. Premi **Informativa (Word)** (nel registro o nella barra laterale) e scegli la categoria: Dipendenti, Clienti, Fornitori, Candidati, Utenti del sito web…
2. Il programma raccoglie tutti i trattamenti **attivi** del registro del titolare che riguardano quella categoria e compone il documento: titolare e contatti, DPO, tabella con finalità, basi giuridiche e conservazione, categorie di dati, natura del conferimento, destinatari, trasferimenti, diritti, reclamo al Garante.
3. Se qualche trattamento si basa sul **consenso**, aggiunge il riquadro per prestarlo o negarlo; in fondo c'è lo spazio per la presa visione.

Più il registro è completo, più l'informativa è precisa. Rileggila sempre prima di consegnarla e, quando l'hai consegnata, metti «Sì» in **Informativa resa** nei trattamenti interessati.

12. Valutazione d'impatto (DPIA)

La DPIA (art. 35 GDPR) è l'analisi scritta da fare **prima** di iniziare un trattamento che può comportare un rischio elevato (videosorveglianza estesa, geolocalizzazione dei dipendenti, dati sanitari su larga scala, dati biometrici, intelligenza artificiale…).

Nuova da trattamento…: scegli il trattamento; il programma compila descrizione, finalità, basi giuridiche, conservazione, responsabili e misure partendo dal registro.

Campo	Cosa scrivere
Descrizione	Natura, ambito e contesto: quali dati, di chi, quanti, come si

	raccolgono, chi li vede.
Necessità e proporzionalità	Risposte alle domande guidate: i dati sono solo quelli necessari? Sono esatti? Per quanto si tengono? Come sono informate le persone e come esercitano i diritti?
Rischi	Per accesso illegittimo, modifica indesiderata e perdita dei dati: minacce, impatti sulle persone, probabilità e gravità. Il livello si calcola da solo.
Misure	Quelle già adottate e quelle da adottare, con tempi e responsabili.
Conclusioni	Parere del DPO, opinione degli interessati (se raccolta), rischio residuo accettabile o no, consultazione del Garante (necessaria se il rischio resta elevato, art. 36), approvazione, prossima revisione.

DPIA in Word produce il documento da firmare e conservare. Dopo averla fatta, metti «Effettuata» nel campo DPIA del trattamento.

13. Registro violazioni (data breach)

Una violazione è qualsiasi evento che porta alla **perdita, distruzione, modifica, divulgazione o accesso non autorizzato** ai dati: un'email inviata alla persona sbagliata, un PC rubato, un attacco informatico, un archivio perso. **Tutte** le violazioni vanno registrate, anche quelle che non si notificano (art. 33.5).

Cosa fare quando succede

1. Registro violazioni › **Nuovo**: inserisci **data e ora** in cui l'hai scoperta. Il programma calcola subito il **termine delle 72 ore** e, in fondo alla scheda, mostra quante ore restano (o da quante è superato).
2. Descrivi cosa è successo, il tipo (riservatezza, integrità, disponibilità), la causa, i trattamenti, i dati e le persone coinvolte.
3. Valuta il rischio per le persone:
    - **Improbabile**: non si notifica, ma scrivi il motivo;
    - **Rischio**: notifica al Garante entro 72 ore;
    - **Rischio elevato**: notifica al Garante e comunicazione agli interessati senza ritardo.
4. Indica lo stato della notifica («Da effettuare» finché non la fai: la riga resta rossa e compare nello scadenzario).
5. La notifica si fa sul sito del Garante con la procedura telematica: il pulsante oro **Notifica al Garante (online)…** nella barra della pagina, oppure quello in fondo alla scheda della violazione, apre direttamente la pagina del Garante. Prepara prima le informazioni della scheda: la procedura le chiede quasi tutte. Poi inserisci data e protocollo e metti «Effettuata».
6. Descrivi le misure adottate e quelle per evitare che si ripeta; quando hai finito metti lo stato «Chiusa».

Stampa PDF produce il registro delle violazioni da conservare.

Il termine di 72 ore e l'indirizzo della procedura del Garante fanno parte del **pacchetto normativo**: se la norma cambia, il programma si aggiorna da solo.

14. Richieste degli interessati

Le persone possono chiedere di accedere ai propri dati, correggerli, cancellarli, limitarne l'uso, riceverli in formato elettronico od opporsi (artt. 15-22).

1. Richieste degli interessati › **Nuovo**: data di ricezione, nome, contatti, diritto esercitato, canale (email, PEC, raccomandata…), contenuto.
2. Verifica l'identità del richiedente e metti «Sì» in **Identità verificata**.
3. Il programma calcola il **termine di risposta**: un mese. Nei casi complessi metti **Proroga** «Sì» (diventa tre mesi) e informa l'interessato entro il primo mese.

4. Quando hai risposto inserisci la data della risposta e l'esito.

Arancione = scade entro 7 giorni; rosso = scaduta senza risposta.

15. Formazione del personale

La formazione di chi tratta i dati è una misura di sicurezza (art. 32) e va documentata.

Campo	Cosa scrivere
Data *, Argomento *	Quando e su cosa (es. «GDPR: regole base e data breach»).
Docente / ente, Modalità, Durata	Chi l'ha tenuta, in presenza o online, quante ore.
Partecipanti	Un nominativo per riga.
Test di verifica	Se c'è stato un test finale.
Prossimo aggiornamento	Di solito dopo un anno: lo scadenzario lo ricorda.

Collega attestati e fogli firme con **Allegati**.

16. Scadenzario

Raccoglie le scadenze di **tutti i titolari** (oppure solo di quello scelto, togliendo la spunta «Tutti i titolari»):

- nomine e contratti in scadenza;
- revisione annuale del registro (dalla data di ultimo aggiornamento) e dei singoli trattamenti;
- revisione delle DPIA e aggiornamento della formazione;
- notifiche delle violazioni entro 72 ore e comunicazioni agli interessati;
- risposte alle richieste degli interessati;
- rinnovo della licenza.

Con **Mostra** puoi vedere solo le scadute o quelle dei prossimi 30 o 90 giorni. Rosso = scaduta, arancione = entro 30 giorni. Doppio clic su una riga per passare a quel titolare. **Stampa PDF** per avere l'elenco su carta.

Consiglio: guardalo una volta alla settimana.

17. Riepilogo conformità

Per ogni titolare il programma esegue una serie di controlli e calcola la **percentuale di conformità**: verde (almeno 90%), arancione (almeno 60%), rosso (sotto il 60%).

Controllo	Come si sistema
Registro compilato	Inserisci almeno un trattamento attivo.
Registro aggiornato negli ultimi 12 mesi	Rivedi il registro e aggiorna la data in Titolari del trattamento o nei trattamenti.
Base giuridica, conservazione, analisi dei rischi, misure di sicurezza	Completa le schede dei trattamenti indicati nel dettaglio.
Condizione art. 9	Nei trattamenti con dati particolari indica la condizione dell'art. 9.2.
Informativa resa	Consegna l'informativa e metti «Sì» nel trattamento.
DPIA dove necessarie	Fai la DPIA dei trattamenti indicati o motiva

	perché non serve.
Nomine firmate e valide	Inserisci la data nomina dei responsabili e rinnova quelle scadute.
Responsabili registrati	Aggiungi in Soggetti e nomine i fornitori citati nei trattamenti.
Autorizzati designati	Inserisci almeno un autorizzato e genera la lettera.
Formazione negli ultimi 12 mesi	Registra un corso.
Violazioni e richieste	Completa le notifiche e le risposte in sospeso.
Dati del DPO	Se il DPO è nominato, indicane il nome.

Dettaglio del titolare (PDF) stampa la verifica del titolare scelto, utile da consegnare al cliente; **Stampa riepilogo PDF** stampa tutti i titolari. Il punteggio aiuta a non dimenticare gli adempimenti principali ma non sostituisce la valutazione di un professionista.

18. Questionario e copia dei trattamenti

Questionario per il cliente (barra laterale, Documenti / Stampa): genera in Word un questionario da inviare al cliente per raccogliere le informazioni: attività svolte, dati particolari, fornitori esterni, strumenti, trasferimenti, misure di sicurezza e situazione attuale. Se è scelto un titolare, i suoi dati sono già compilati.

Copia trattamenti…: copia i trattamenti scelti dal titolare attuale a un altro (utile per clienti con attività simili). I responsabili esterni e i contitolari non vengono copiati perché appartengono al titolare di origine: vanno indicati nel nuovo titolare.

19. Procedure rapide

Nuovo cliente (per gli studi)

1. Titolari del trattamento › Nuovo.
2. Questionario per il cliente.
3. Trattamenti da modello o copiati da un cliente simile.
4. Soggetti, nomine e informative.
5. Riepilogo conformità e stampa del registro.

Revisione annuale

1. Apri ogni trattamento, aggiorna ciò che è cambiato e la data di ultima revisione.
2. Controlla nomine e formazione nello Scadenzario.
3. Aggiorna la data in Titolari del trattamento › Data ultimo aggiornamento del registro.
4. Ristampa il registro.

È successa una violazione

1. Registro violazioni › Nuovo con data e ora della scoperta.
2. Valuta il rischio.
3. Se serve, notifica al Garante entro le 72 ore indicate, con il pulsante **Notifica al Garante (online)…**.
4. Chiudi la violazione con le misure adottate.

Una persona chiede i suoi dati

1. Richieste degli interessati › Nuovo.
2. Verifica l'identità.
3. Rispondi entro il termine indicato e registra data ed esito.

Cambio PC

1. Sul vecchio PC: Sistema › Backup e ripristino › Backup archivio su una chiavetta.
2. Sul nuovo PC: installa il programma, attiva la licenza con lo stesso codice.
3. Sistema › Backup e ripristino › Ripristina backup.

Lavorare in ufficio e a casa

1. Imposta Sync cloud con la cartella di Drive su entrambi i PC.
2. A fine giornata in ufficio: Condividi.
3. A casa: Importa, lavora, Condividi.

Non trovo come si fa una cosa

1. Cerca una parola in questa guida (casella in alto).
2. Guarda le Domande frequenti.
3. Chiedi all'**Assistente Korevium Privacy** (pulsante Assistente in alto).
4. Se serve, scrivi all'assistenza (Sistema › Assistenza).

Aggiornare il programma

1. Pulsante Aggiornamenti › Scarica.
2. Fai un backup.
3. Chiudi il programma ed esegui il file scaricato.

20. Pacchetto normativo

Il **pacchetto normativo** è la parte del programma che contiene le regole: le norme di riferimento, i termini (ad esempio le 72 ore per notificare una violazione, il mese per rispondere agli interessati), gli elenchi proposti nelle maschere (basi giuridiche, categorie di dati, misure di sicurezza, criteri della DPIA), i modelli dei trattamenti e i testi dei documenti Word.

Perché è separato dal programma: le norme sulla protezione dei dati cambiano nel tempo, soprattutto per effetto di provvedimenti del Garante, linee guida europee e modifiche legislative. Con il pacchetto normativo il programma si adegua senza essere reinstallato.

Come si aggiorna

1. Korevium pubblica il nuovo pacchetto sul sito, **firmato digitalmente**: il programma accetta solo pacchetti con una firma valida, quindi nessuno può alterare le regole.
2. Il controllo degli aggiornamenti (all'avvio, oppure pulsante **Aggiornamenti**) lo scarica e ne verifica la firma.
3. Il pacchetto si applica dalla sua **data di entrata in vigore**, al primo avvio del programma da quel giorno. Se arriva prima, resta «in attesa».
4. Al primo avvio con il pacchetto nuovo compare l'elenco di cosa è cambiato. Se sono cambiati i testi dei documenti, il programma invita a **rigenerare informative e nomine**: quelle già stampate riportano i testi precedenti.

Sistema › Pacchetto normativo mostra la versione in uso, le norme di riferimento, i valori applicati e l'eventuale pacchetto in attesa. Il pulsante **Salva PDF** ne conserva una copia, utile come prova delle regole applicate in un certo periodo.

I dati già inseriti non vengono modificati dal pacchetto: cambiano gli elenchi proposti, i calcoli dei termini e i testi dei documenti generati da quel momento.

21. Assistente Korevium Privacy

L'**Assistente Korevium Privacy** è una chat sul sito, istruita su questa guida e sull'uso del programma. Si apre dal pulsante **Assistente** nella barra in alto oppure da **Sistema › Assistente Korevium Privacy**: il programma apre il browser alla pagina dell'assistente.

Cosa chiedere: come si fa un'operazione («come genero la nomina del consulente del lavoro?»), cosa significa un campo o un avviso («perché mi dice che la DPIA è necessaria?»), cosa prevede la

disciplina («entro quando rispondo a una richiesta di cancellazione?»), dove si trova una funzione.

Cosa non scrivere: dati personali di terzi, cioè nomi, codici fiscali o dettagli di clienti, dipendenti o interessati. Descrivi il caso in termini generali («un dipendente ha inviato un file con dati di clienti a un indirizzo sbagliato»).

Le risposte sono indicazioni generali: nei casi complessi, o quando c'è una scelta di merito da fare, resta il parere del consulente privacy o del DPO. Per problemi tecnici del programma usa **Sistema › Assistenza**.

22. Database e uso in rete

Dove sono i dati: nel file **privacy.db**. Gli allegati sono nella cartella **allegati** accanto al database. Il percorso è indicato in Sistema › Informazioni.

Sistema › Cartella del database permette di spostare il database su un'altra cartella del PC, su un disco di rete o su un NAS dell'ufficio. Il programma copia database e allegati e si chiude: alla riapertura usa la nuova cartella.

Uso da più PC in ufficio: con il database su un disco di rete o NAS, più PC possono usarlo, ma uno alla volta. Se è già aperto altrove il programma avvisa e permette di aprirlo in sola lettura.

Uso da più PC in luoghi diversi (ufficio e casa, più sedi): usare **Sync cloud** (vedi la sezione dedicata). Non spostare i dati copiando o sincronizzando a mano la cartella di lavoro.

23. Backup e ripristino

Sistema › Backup e ripristino apre la finestra per salvare e recuperare l'archivio. Il backup è un **file zip completo**: database e allegati.

Backup automatico: se è attivo, il programma salva uno zip nella **cartella a chiusura** (pulsante **Apri** per vederla), alla chiusura del programma oppure una volta al giorno (campo **Frequenza**). **Copie da conservare** tiene gli ultimi zip (massimo 20) e cancella i più vecchi.

Backup manuale: indicare la **cartella backup manuale** (meglio una chiavetta, un disco esterno o di rete) e premere **Backup archivio**. Conviene farlo periodicamente: se il PC si guasta, i backup sullo stesso disco andrebbero persi insieme ai dati.

Ripristino: premere **Ripristina backup** e scegliere il file (zip, oppure un vecchio file .db). Il programma mostra data, titolari e allegati contenuti nel backup e chiede conferma. Prima di ripristinare salva automaticamente un **backup di sicurezza** dei dati attuali, poi controlla l'integrità del file e sostituisce database e allegati con quelli del backup.

Salva impostazioni memorizza le scelte della finestra.

24. Sync cloud

Sistema › Sync cloud permette di lavorare sullo stesso archivio da più PC, anche in luoghi diversi, usando una cartella di Google Drive, OneDrive o simili. Si lavora sempre **in locale**: sul Drive resta un solo file per archivio (database e allegati), **bloccato** mentre un computer lo sta usando. Così i dati non si danneggiano.

Come si usa

1. A destra, indicare la **cartella Drive** (Sfoglia…) e premere 💾 **Salva**.
2. Sul PC dove ci sono i dati, indicare il nome dell'archivio e premere **Condividi** →: l'archivio viene pubblicato sul Drive e i dati su quel PC vengono svuotati.
3. Sul PC dove si vuole lavorare, selezionare l'archivio a destra e premere ← **Importa**: i dati arrivano sul PC e sul Drive l'archivio diventa **FREEZE** (bloccato, sola lettura per gli altri PC).
4. A fine lavoro premere di nuovo **Condividi** →: l'archivio torna disponibile per gli altri PC.

Forza: spuntarlo per importare sovrascrivendo i dati già presenti sul PC, oppure per usare **Forza sblocco**, che sblocca un archivio rimasto in FREEZE (ad esempio se un PC si è guastato prima di

condividere). Usare lo sblocco solo se si è sicuri che nessuno ci stia lavorando.

I dati copiati sul Drive sono custoditi dal servizio cloud scelto dall'utente: il programma non li invia altrove.

25. Licenza e versione dimostrativa

Senza licenza il programma funziona in **versione dimostrativa**: 1 titolare, 5 trattamenti, stampe con la scritta «VERSIONE DIMOSTRATIVA».

Per attivare la licenza: **Sistema › Licenza**, premere **Richiedi la licenza…** (prepara un'email da completare con intestatario e partita IVA) oppure contattare l'assistenza. Il codice di attivazione ricevuto va incollato nella finestra Licenza (oppure caricato dal file .key) e confermato con **Attiva**; poi riavviare il programma.

Più PC: la licenza è intestata alla **partita IVA** e vale su tutti i PC dell'intestatario. Su ogni PC basta incollare lo stesso codice di attivazione.

Edizione Mono: gestisce solo il titolare del trattamento intestatario della licenza, che deve avere la stessa partita IVA o lo stesso codice fiscale.

Edizioni: Mono (1 titolare) e Multi (titolari illimitati: imprese, studi, professionisti, enti).

Scadenza: la licenza è annuale. Un mese prima compare l'avviso in alto. Alla scadenza il programma resta consultabile e stampabile, ma non si possono modificare i dati fino al rinnovo.

Cambio PC: sul nuovo PC basta attivare lo stesso codice di attivazione.

26. Aggiornamenti

Pulsante **Aggiornamenti** in alto a destra (oppure **Sistema › Aggiornamenti**): il programma controlla sul sito se c'è una versione più recente e, se c'è, mostra le novità e il pulsante **Scarica**.

La verifica avviene anche automaticamente a ogni apertura del programma. Si può disattivare togliendo la spunta da **Controlla gli aggiornamenti all'avvio**, in fondo alla pagina Sistema.

Pacchetto normativo: con lo stesso controllo il programma scarica, quando c'è, il pacchetto normativo aggiornato (elenchi, termini e testi dei documenti adeguati alle nuove norme). È firmato digitalmente da Korevium e si applica da solo, senza reinstallare, dalla data di entrata in vigore. Versione e modifiche: **Sistema › Pacchetto normativo**.

La verifica scarica solo un piccolo file: il programma non invia alcun dato.

Per installare l'aggiornamento chiudere il programma ed eseguire il file scaricato: i dati non vengono cancellati. Prima di aggiornare è comunque buona norma fare un backup.

27. Assistenza

Sistema › Assistenza mostra i contatti e gli orari. Il pulsante **Scrivi all'assistenza** prepara un'email con la versione del programma e il codice del PC, da completare con la descrizione del problema.

Se necessario l'assistenza può collegarsi al PC con **AnyDesk**, solo con il consenso dell'utente.

Assistente Korevium Privacy

Il pulsante **Assistente** nella barra in alto (oppure **Sistema › Assistente Korevium Privacy**) apre nel browser la pagina **www.denacommercialistaonline.it/assistente-korevium-privacy**. È una chat istruita sulla guida e sull'uso del programma: risponde a domande come «come genero la nomina del consulente del lavoro?», «quando serve la DPIA?» o «cosa devo fare entro le 72 ore?». È disponibile a qualsiasi ora.

Le risposte dell'assistente sono indicazioni generali: per i casi particolari resta il parere di un professionista. Nella chat non inserire dati personali di terzi (nomi di clienti, dipendenti, interessati): descrivi la situazione in termini generali.

28. La disciplina: le fonti e come leggerle

Questa seconda parte della guida spiega, in modo discorsivo ma preciso, le regole che il programma aiuta ad applicare. Non sostituisce la lettura delle norme né il parere di un professionista, ma permette di capire **perché** il programma chiede un'informazione o propone un adempimento.

Le fonti principali

- **Regolamento (UE) 2016/679 (GDPR)**: è direttamente applicabile in tutti gli Stati dell'Unione dal 25 maggio 2018. Contiene i principi, i diritti degli interessati, gli obblighi di titolari e responsabili e le sanzioni. Gli articoli sono preceduti da 173 «considerando», utili a interpretarli.
- **D.Lgs. 196/2003 (Codice privacy)**, come modificato dal D.Lgs. 101/2018: adegua l'ordinamento italiano al GDPR e disciplina gli spazi lasciati agli Stati (ad esempio le persone autorizzate, art. 2-quaterdecies; il consenso dei minori, art. 2-quinquies; i dati relativi alla salute, genetici e biometrici, art. 2-septies; i dati giudiziari, art. 2-octies; il lavoro, artt. 113-114; gli illeciti penali, artt. 167 e seguenti).
- **Provvedimenti e linee guida del Garante**: indicano come applicare le regole in casi concreti (amministratori di sistema, videosorveglianza, cookie, data breach, elenco dei trattamenti soggetti a DPIA).
- **Linee guida dell'EDPB** (Comitato europeo per la protezione dei dati): interpretazioni comuni a tutte le autorità europee, ad esempio sulla DPIA (WP248), sui data breach (9/2022), sulla videosorveglianza (3/2019).
- **Norme di settore** che si intrecciano con la privacy: lo Statuto dei lavoratori (art. 4, L. 300/1970) per i controlli a distanza, il codice civile per la conservazione delle scritture contabili (art. 2220 c.c.), le norme fiscali, antiriciclaggio e sanitarie per i tempi e le basi giuridiche dei trattamenti.

L'elenco aggiornato delle norme che il programma applica è in **Sistema › Pacchetto normativo**.

29. La disciplina: principi e responsabilizzazione

Tutto il GDPR ruota intorno ai **principi dell'art. 5**. I dati personali devono essere:

- **trattati in modo lecito, corretto e trasparente** (liceità, correttezza, trasparenza);
- **raccolti per finalità determinate, esplicite e legittime** e non usati poi in modo incompatibile (limitazione della finalità);
- **adeguati, pertinenti e limitati** a quanto necessario (minimizzazione);
- **esatti e aggiornati** (esattezza);
- **conservati per il tempo necessario** e poi cancellati o resi anonimi (limitazione della conservazione);
- **protetti** da accessi non autorizzati, perdita o distruzione (integrità e riservatezza).

A questi si aggiunge il principio di **responsabilizzazione** (accountability, artt. 5.2 e 24): il titolare non deve solo rispettare le regole, ma **essere in grado di dimostrarlo**. È la ragione per cui servono un registro, documenti firmati, analisi dei rischi, prove della formazione: in caso di controllo o di reclamo, è il titolare a dover provare di aver agito correttamente.

Protezione fin dalla progettazione e per impostazione predefinita (art. 25): quando si sceglie un nuovo programma, un servizio cloud o una procedura, bisogna pensare subito a quali dati servono davvero, chi deve vederli e per quanto tempo tenerli, e configurare tutto in modo che di default si trattino solo i dati necessari.

Nel programma: ogni scheda del trattamento traduce questi principi in campi concreti (finalità, base giuridica, categorie di dati, conservazione, misure). Il Riepilogo conformità, gli allegati e lo scadenzario sono gli strumenti della responsabilizzazione.

30. La disciplina: i ruoli

Titolare del trattamento (art. 4, n. 7; art. 24)

È il soggetto che **decide le finalità e i mezzi** del trattamento: l'impresa per i dati dei propri

dipendenti e clienti, lo studio per i propri, l'ente per i suoi. Risponde del rispetto delle regole e lo deve dimostrare. Nelle società il titolare è la società stessa, non il legale rappresentante, che però firma i documenti in suo nome.

Contitolari (art. 26)

Quando due o più soggetti decidono **insieme** finalità e mezzi (ad esempio due società che organizzano un evento comune raccogliendo iscrizioni) sono contitolari: devono stipulare un accordo che ripartisca gli obblighi, e il contenuto essenziale dell'accordo va messo a disposizione degli interessati.

Responsabile del trattamento (art. 28)

È chi tratta i dati **per conto del titolare**: il consulente del lavoro che elabora le buste paga, il commercialista che tiene la contabilità, il fornitore del gestionale in cloud, la ditta che gestisce le telecamere. Il titolare deve scegliere responsabili che offrano garanzie sufficienti e vincolarli con un **contratto o altro atto giuridico** con i contenuti dell'art. 28.3: oggetto, durata, natura e finalità, tipo di dati, istruzioni, riservatezza, sicurezza, assistenza al titolare, sorte dei dati alla fine del rapporto, possibilità di verifiche. Il responsabile può ricorrere a un altro responsabile (sub-responsabile) solo con l'autorizzazione scritta del titolare (art. 28.2 e 28.4).

Persone autorizzate (art. 29; art. 2-quaterdecies Codice)

Dipendenti e collaboratori che trattano dati sotto l'autorità del titolare devono ricevere **istruzioni**. Il Codice consente al titolare di attribuire specifici compiti a persone designate: è la lettera di autorizzazione che il programma genera.

Amministratori di sistema

Chi gestisce server, reti, banche dati e sistemi (interno o esterno) va designato individualmente per iscritto, dopo averne valutato esperienza e affidabilità. Il provvedimento del Garante del 27 novembre 2008 richiede tra l'altro la registrazione degli accessi logici degli amministratori, conservata per almeno sei mesi, e una verifica almeno annuale del loro operato.

Responsabile della protezione dei dati - DPO (artt. 37-39)

È obbligatorio per autorità e organismi pubblici e per chi, come attività principale, effettua un **monitoraggio regolare e sistematico su larga scala** o tratta **su larga scala** dati particolari o giudiziari. Negli altri casi è facoltativo. Il DPO consiglia e sorveglia, deve essere indipendente e i suoi dati di contatto vanno comunicati al Garante e indicati nelle informative.

Rappresentante nell'Unione (art. 27)

Serve ai titolari stabiliti fuori dall'UE che offrono beni o servizi a persone nell'Unione o ne monitorano il comportamento.

31. La disciplina: il doppio ruolo degli studi professionali

Commercialisti, consulenti del lavoro, avvocati e altri professionisti hanno spesso **due ruoli**:

- **titolari** per i dati che trattano per sé: dipendenti e collaboratori dello studio, anagrafica e fatturazione dei clienti, fornitori, sito web;
- **responsabili** per i dati che trattano per conto dei clienti, ad esempio i dati dei dipendenti del cliente elaborati per le buste paga, o i dati di clienti e fornitori del cliente registrati in contabilità.

La qualificazione dipende dal caso concreto: quando il professionista decide autonomamente come trattare i dati per adempiere a un proprio obbligo professionale può essere egli stesso titolare. È una valutazione da fare, e documentare, per ciascun tipo di incarico.

Cosa significa in pratica

1. Lo studio tiene il proprio **registro del titolare** (art. 30.1).
2. Per i trattamenti svolti per conto dei clienti tiene il **registro del responsabile** (art. 30.2),

indicando per ciascuno il cliente per conto del quale tratta i dati.
3. Ogni cliente deve aver nominato lo studio **responsabile** (art. 28): spesso è lo studio stesso a proporre l'atto di nomina.
4. Lo studio deve autorizzare il proprio personale e, se usa fornitori (software in cloud, conservazione digitale), designarli come sub-responsabili con l'autorizzazione dei clienti.

Nel programma: lo studio si inserisce come titolare; con l'edizione Multi ogni cliente è un titolare distinto, di cui lo studio può curare registro, nomine e informative. Nella scheda del trattamento il campo «Registro» distingue titolare (art. 30.1) e responsabile (art. 30.2).

32. La disciplina: basi giuridiche e categorie particolari

Ogni trattamento deve fondarsi su una delle **basi giuridiche dell'art. 6**:

- **consenso** dell'interessato (lett. a);
- **esecuzione di un contratto** o di misure precontrattuali richieste dall'interessato (lett. b);
- **obbligo di legge** a cui è soggetto il titolare (lett. c);
- **interessi vitali** dell'interessato o di un'altra persona (lett. d);
- **interesse pubblico** o esercizio di pubblici poteri (lett. e);
- **legittimo interesse** del titolare o di terzi, se non prevalgono i diritti dell'interessato (lett. f).

Il consenso non è la regola: per pagare uno stipendio, emettere una fattura o tenere la contabilità la base è il contratto o l'obbligo di legge, e chiedere un consenso sarebbe scorretto (non potrebbe essere rifiutato liberamente). Il consenso serve, ad esempio, per marketing diretto via email a chi non è cliente, newsletter, profilazione a fini commerciali. Quando è la base, deve essere libero, specifico, informato e inequivocabile, va documentato e si può revocare in qualsiasi momento (art. 7). Per i servizi online offerti direttamente ai minori, in Italia il minore può consentire da solo dai 14 anni (art. 2-quinquies Codice).

Legittimo interesse: richiede un bilanciamento documentato tra l'interesse del titolare (sicurezza, tutela del credito, prevenzione delle frodi) e i diritti e le ragionevoli aspettative dell'interessato. Va descritto nel campo dedicato del trattamento e indicato nell'informativa.

Categorie particolari (art. 9) e dati giudiziari (art. 10)

Salute, origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici e biometrici, vita od orientamento sessuale: il loro trattamento è **vietato** salvo che ricorra una delle condizioni dell'art. 9.2 (ad esempio obblighi in materia di lavoro e sicurezza sociale, medicina del lavoro, consenso esplicito, difesa di un diritto in giudizio). Per salute, dati genetici e biometrici il Codice prevede inoltre misure di garanzia (art. 2-septies). I dati su condanne penali e reati si trattano solo se una norma lo consente (art. 10; art. 2-octies Codice).

Nel programma: la scheda Finalità chiede base giuridica e legittimo interesse; la scheda Interessati e dati chiede le categorie particolari e la relativa condizione dell'art. 9.2. Se indichi dati particolari senza condizione, l'avviso giallo lo segnala.

33. La disciplina: informative e trasparenza

Le persone hanno diritto di sapere chi tratta i loro dati, perché e come (artt. 12-14). L'informativa deve essere **concisa, trasparente, intelligibile e facilmente accessibile**, con un linguaggio semplice.

Quando si dà

- **Dati raccolti presso l'interessato** (art. 13): nel momento in cui i dati sono raccolti (alla firma del contratto, all'assunzione, alla compilazione del modulo sul sito).
- **Dati ottenuti da altri** (art. 14): entro un termine ragionevole e al più tardi entro un mese, oppure alla prima comunicazione con l'interessato o alla prima comunicazione dei dati a terzi.

Cosa deve contenere

Identità e contatti del titolare e dell'eventuale DPO; finalità e base giuridica di ogni trattamento (e il

legittimo interesse, se è la base); destinatari o categorie di destinatari; eventuali trasferimenti fuori dall'UE e relative garanzie; periodo di conservazione o criteri per determinarlo; diritti dell'interessato, incluso il reclamo al Garante; se il conferimento è obbligatorio e cosa accade se si rifiuta; l'eventuale esistenza di decisioni automatizzate. Per i dati ottenuti da altri vanno indicate anche le categorie di dati e la fonte.

Videosorveglianza: oltre all'informativa completa serve un **cartello** visibile prima di entrare nell'area ripresa, con le informazioni essenziali e l'indicazione di dove trovare l'informativa completa.

Nel programma: Informativa (Word) raccoglie automaticamente i trattamenti che riguardano la categoria di interessati scelta e compone il testo con finalità, basi giuridiche, conservazione, destinatari, trasferimenti e diritti. Va sempre riletta e adattata prima della consegna. Nel trattamento, il campo «Informativa resa» serve al Riepilogo conformità.

34. La disciplina: i diritti degli interessati

L'interessato può esercitare i diritti degli artt. 15-22:

- **accesso** (art. 15): sapere se e quali dati sono trattati e averne copia;
- **rettifica** (art. 16): correggere dati inesatti o incompleti;
- **cancellazione** (art. 17, «diritto all'oblio»): nei casi previsti, ad esempio quando i dati non servono più o il consenso è revocato; non si applica se il titolare deve conservarli per legge;
- **limitazione** (art. 18): «congelare» i dati mentre si verifica una contestazione;
- **portabilità** (art. 20): ricevere in formato strutturato i dati forniti, se il trattamento si basa su consenso o contratto ed è automatizzato;
- **opposizione** (art. 21): in particolare al trattamento basato sul legittimo interesse e, sempre, al marketing diretto;
- **non essere sottoposto a decisioni solo automatizzate** con effetti significativi (art. 22).

Termini e modalità (art. 12)

Il titolare risponde **senza ingiustificato ritardo e comunque entro un mese** dal ricevimento della richiesta. Il termine può essere **prorogato di due mesi** se necessario, tenuto conto della complessità e del numero delle richieste, informando l'interessato della proroga e dei motivi entro il primo mese. La risposta è gratuita, salvo richieste manifestamente infondate o eccessive. Il titolare può chiedere informazioni per verificare l'identità del richiedente. Se non intende dare seguito alla richiesta, deve spiegarne i motivi e informare della possibilità di reclamo al Garante o di ricorso al giudice. Il Codice prevede alcune limitazioni ai diritti in casi specifici (art. 2-undecies).

Nel programma: Richieste degli interessati calcola il termine (con o senza proroga), lo inserisce nello scadenzario e registra risposta ed esito. Il registro delle richieste è una prova utile della gestione corretta.

35. La disciplina: sicurezza e analisi dei rischi

L'art. 32 non elenca misure obbligatorie uguali per tutti: chiede misure tecniche e organizzative **adeguate al rischio**, tenendo conto dello stato dell'arte, dei costi, della natura e del contesto del trattamento e della probabilità e gravità dei rischi per le persone. Tra gli esempi indicati dalla norma: pseudonimizzazione e cifratura; capacità di assicurare riservatezza, integrità, disponibilità e resilienza dei sistemi; capacità di ripristinare tempestivamente i dati dopo un incidente; procedure per testare e valutare periodicamente l'efficacia delle misure.

Come si ragiona sul rischio

Il rischio va valutato dal punto di vista delle **persone** a cui si riferiscono i dati, non dell'azienda: cosa succederebbe a un dipendente se i suoi dati sanitari finissero in mano a terzi? Si combinano due fattori:

- **probabilità** che un evento accada (accesso non autorizzato, perdita, modifica indesiderata);
- **gravità** delle conseguenze per le persone (disagio, danno economico, discriminazione, danno reputazionale).

Il **rischio inerente** è quello prima delle misure; il **rischio residuo** quello che resta dopo. L'obiettivo è portare il rischio residuo a un livello accettabile.

Misure tipiche per una piccola organizzazione

- credenziali personali e robuste, autenticazione a due fattori per posta e servizi cloud;
- aggiornamenti regolari, antivirus, firewall;
- backup periodici, conservati anche fuori sede, e prove di ripristino;
- profili di accesso: ognuno vede solo i dati che gli servono;
- cifratura di portatili e chiavette;
- armadi chiusi, scrivania pulita, distruzione sicura dei documenti;
- istruzioni scritte e **formazione** del personale: chi tratta i dati deve farlo secondo le istruzioni del titolare (artt. 29 e 32.4), e la formazione è una misura organizzativa decisiva perché la maggior parte degli incidenti nasce da errori umani.

Nel programma: la scheda Analisi dei rischi di ogni trattamento calcola rischio inerente e residuo; le misure si spuntano nella scheda Conservazione e sicurezza; la Formazione ha un suo registro.

36. La disciplina: valutazione d'impatto (DPIA) e consultazione preventiva

La **valutazione d'impatto sulla protezione dei dati** (art. 35) è obbligatoria quando un trattamento, specie se usa nuove tecnologie, **può presentare un rischio elevato** per i diritti e le libertà delle persone. Va fatta **prima** di iniziare il trattamento.

Quando è necessaria

Il GDPR indica tre casi certi: valutazione sistematica e globale di aspetti personali con decisioni che producono effetti giuridici (profilazione); trattamento su larga scala di dati particolari o giudiziari; sorveglianza sistematica su larga scala di zone accessibili al pubblico. Oltre a questi, le linee guida WP248 individuano **nove criteri**: valutazione o scoring, decisioni automatizzate, monitoraggio sistematico, dati sensibili o molto personali, larga scala, combinazione di insiemi di dati, interessati vulnerabili (tra cui i dipendenti), uso innovativo di tecnologie, trattamenti che impediscono di esercitare un diritto o accedere a un servizio. **Con due o più criteri la DPIA è di norma necessaria**. Il Garante ha pubblicato un elenco di dodici tipologie di trattamento per cui è richiesta (provv. n. 467 dell'11 ottobre 2018), che non è esaustivo: tra queste i trattamenti nel rapporto di lavoro con sistemi tecnologici che consentono il monitoraggio dei dipendenti (come videosorveglianza e geolocalizzazione), i trattamenti di dati biometrici e genetici, i trattamenti su larga scala di dati di soggetti vulnerabili e l'uso di tecnologie innovative, come l'intelligenza artificiale, insieme ad almeno un altro criterio.

Cosa contiene (art. 35.7)

1. descrizione sistematica del trattamento e delle finalità;
2. valutazione della necessità e proporzionalità;
3. valutazione dei rischi per i diritti e le libertà degli interessati;
4. misure previste per affrontare i rischi e dimostrare la conformità.

Se è stato designato un DPO, il titolare ne raccoglie il parere; quando opportuno, raccoglie anche l'opinione degli interessati o dei loro rappresentanti. La DPIA va riesaminata quando cambiano i rischi.

Consultazione preventiva (art. 36)

Se, nonostante le misure, il rischio residuo resta elevato, il titolare deve **consultare il Garante prima** di iniziare il trattamento. Il Garante si esprime di norma entro otto settimane, prorogabili di sei.

Nel programma: la DPIA si crea da un trattamento (Nuova da trattamento…), è guidata nelle sezioni previste dall'art. 35.7 e si esporta in Word.

37. La disciplina: violazioni dei dati (data breach)

Una **violazione dei dati personali** (art. 4, n. 12) è una 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. Si distinguono violazioni di **riservatezza** (accesso o divulgazione), **integrità** (modifica) e **disponibilità** (perdita o indisponibilità, anche temporanea, ad esempio per un ransomware).

I tre obblighi

1. **Documentare sempre** (art. 33.5): ogni violazione va annotata nel registro, con fatti, effetti e provvedimenti adottati, anche quando non si notifica.
2. **Notificare al Garante** (art. 33) **senza ingiustificato ritardo e, ove possibile, entro 72 ore** dal momento in cui se ne è venuti a conoscenza, salvo che sia improbabile che la violazione presenti un rischio per le persone. Oltre le 72 ore la notifica va accompagnata dai motivi del ritardo. Se non tutte le informazioni sono disponibili si può notificare per fasi. Dal 1° luglio 2021 la notifica si fa esclusivamente con la **procedura telematica** del Garante. Il responsabile del trattamento che scopre una violazione deve informare il titolare senza ingiustificato ritardo.
3. **Comunicare agli interessati** (art. 34) senza ingiustificato ritardo quando il rischio è **elevato**, con linguaggio semplice, descrivendo la violazione, le conseguenze probabili, le misure adottate e i contatti. Non serve se i dati erano cifrati e illeggibili, se le misure successive hanno eliminato il rischio elevato o se richiederebbe sforzi sproporzionati (in tal caso si ricorre a una comunicazione pubblica).

«Conoscenza» significa ragionevole certezza che un incidente di sicurezza abbia compromesso dati personali: un breve periodo di indagine è ammesso, ma non può diventare un modo per rinviare il termine.

Le linee guida EDPB 9/2022 contengono numerosi esempi pratici (email inviata al destinatario sbagliato, ransomware con o senza backup, furto di un portatile cifrato o non cifrato) con l'indicazione di quando notificare e comunicare.

Nota: è in discussione a livello europeo una proposta (il cosiddetto «Digital Omnibus») che porterebbe il termine a 96 ore e limiterebbe la notifica ai casi di rischio elevato. Finché non è approvata valgono le regole attuali; se cambieranno, il pacchetto normativo aggiornerà da solo termini e testi del programma.

Nel programma: Registro violazioni calcola il termine, mostra le ore che restano, apre la procedura del Garante e conserva il registro completo.

38. La disciplina: conservazione dei dati

I dati vanno conservati **per il tempo necessario** alle finalità (art. 5.1.e). Il titolare deve stabilire per ogni trattamento un termine, o almeno il criterio per determinarlo, e indicarlo nel registro e nell'informativa. Scaduto il termine, i dati vanno cancellati o resi anonimi.

Spesso il termine deriva da altre norme: ad esempio le scritture contabili e la relativa documentazione si conservano per dieci anni (art. 2220 c.c.); i documenti di lavoro seguono i termini previdenziali e di prescrizione; per l'antiriciclaggio valgono i termini propri di quella disciplina. Quando nessuna norma fissa un termine, va scelto un periodo ragionevole e motivato (ad esempio per i curricula non selezionati).

Per le immagini della videosorveglianza i tempi devono essere brevi: le linee guida EDPB 3/2019 indicano che di norma bastano pochi giorni e che conservazioni oltre le 72 ore richiedono una motivazione specifica.

Nel programma: il campo «Termine di conservazione» propone i termini più frequenti, il campo «Criterio / note» ne spiega la ragione; entrambi finiscono nell'informativa.

39. La disciplina: lavoratori, videosorveglianza e geolocalizzazione

I dati dei lavoratori sono trattati con continuità e in un rapporto squilibrato: per questo la disciplina è più rigorosa (art. 88 GDPR; artt. 113-114 Codice).

Controlli a distanza (art. 4 L. 300/1970)

Impianti audiovisivi e altri strumenti da cui derivi anche la possibilità di controllo a distanza dei lavoratori (telecamere, sistemi di geolocalizzazione dei veicoli, alcuni software) possono essere usati **solo** per esigenze organizzative e produttive, sicurezza del lavoro o tutela del patrimonio, e installati **previo accordo sindacale** o, in mancanza, **autorizzazione dell'Ispettorato del lavoro**. Non serve l'accordo per gli strumenti usati per rendere la prestazione lavorativa e per quelli di registrazione di accessi e presenze. In ogni caso il lavoratore deve ricevere adeguata informazione sulle modalità d'uso degli strumenti e sui controlli, nel rispetto del GDPR. Violare queste regole può costituire anche reato (art. 171 Codice).

Videosorveglianza

Servono finalità chiare, angolazioni limitate allo stretto necessario, cartello e informativa, tempi di conservazione brevi, accesso alle immagini riservato a persone autorizzate, nomina della ditta che gestisce l'impianto come responsabile. Se le telecamere riprendono i lavoratori occorre la procedura dell'art. 4 dello Statuto. In molti casi (monitoraggio sistematico, dipendenti come interessati vulnerabili) va valutata la DPIA.

Geolocalizzazione

Il GPS su veicoli aziendali rientra di norma tra gli strumenti di controllo dell'art. 4: servono accordo o autorizzazione, informativa specifica, limitazione dei dati e dei tempi e, di regola, la DPIA.

Posta elettronica e internet

Il datore di lavoro può dettare regole sull'uso degli strumenti, ma non può effettuare controlli prolungati, costanti o indiscriminati sulla posta e sulla navigazione dei dipendenti. Le regole vanno messe per iscritto in un disciplinare interno e comunicate.

40. La disciplina: trasferimenti fuori dall'Unione europea

I dati possono essere trasferiti verso paesi fuori dallo Spazio economico europeo (paesi terzi) solo alle condizioni degli artt. 44-49:

- **decisione di adeguatezza** della Commissione (art. 45): il paese assicura un livello di protezione adeguato. Per gli Stati Uniti vale il **Data Privacy Framework** (decisione (UE) 2023/1795 del 10 luglio 2023), ma solo verso le organizzazioni americane che vi hanno aderito: va verificato nell'elenco ufficiale. La decisione è stata confermata dal Tribunale dell'UE il 3 settembre 2025 ed è oggetto di impugnazione davanti alla Corte di giustizia;
- **garanzie adeguate** (art. 46), come le clausole contrattuali standard della Commissione, accompagnate da una valutazione del contesto del paese di destinazione;
- **norme vincolanti d'impresa** per i gruppi (art. 47);
- **deroghe** per situazioni specifiche (art. 49), da usare in modo restrittivo.

Molti servizi di uso comune (posta, cloud, videoconferenza, newsletter) comportano trasferimenti: va verificato nei contratti dove sono trattati i dati e su quale base.

Nel programma: nella scheda Destinatari del trattamento si indicano paesi terzi e garanzie; l'informativa e la nomina del responsabile ne tengono conto.

41. La disciplina: sanzioni e responsabilità

Sanzioni amministrative (art. 83)

Il Garante può infliggere sanzioni fino a **10 milioni di euro o al 2% del fatturato mondiale annuo** (se superiore) per le violazioni degli obblighi organizzativi: registro, sicurezza, notifica delle violazioni, DPIA, nomine dei responsabili, DPO. Fino a **20 milioni di euro o al 4%** per le violazioni dei principi, delle basi giuridiche, dei diritti degli interessati, dei trasferimenti e degli ordini del Garante. La sanzione tiene conto di natura, gravità e durata della violazione, del carattere doloso o colposo, delle misure adottate per attenuare il danno, del grado di cooperazione e delle precedenti violazioni: avere la documentazione in ordine pesa nella valutazione.

Poteri correttivi (art. 58)

Il Garante può anche ammonire, ordinare di conformarsi, limitare o vietare un trattamento, ordinare la cancellazione dei dati: provvedimenti che possono incidere sull'attività più della sanzione stessa.

Risarcimento del danno (art. 82)

Chi subisce un danno materiale o immateriale da una violazione del GDPR ha diritto al risarcimento dal titolare o dal responsabile, che si libera solo provando che l'evento non gli è in alcun modo imputabile.

Illeciti penali (artt. 167 e seguenti Codice)

Il Codice punisce, tra l'altro, il trattamento illecito di dati al fine di trarne profitto o di arrecare danno, la comunicazione e diffusione illecita di dati su larga scala, le false dichiarazioni al Garante, l'inosservanza dei suoi provvedimenti e la violazione delle regole sui controlli a distanza dei lavoratori.

42. La disciplina: tenere tutto in ordine nel tempo

La protezione dei dati non è un adempimento da fare una volta: è un sistema da mantenere. Una buona routine:

- **a ogni cambiamento** (nuovo fornitore, nuovo software, nuova attività, telecamere, nuovo sito): aggiornare il registro, valutare i rischi e, se serve, la DPIA; nominare i nuovi responsabili; aggiornare le informative;
- **a ogni nuovo dipendente o collaboratore**: informativa, lettera di autorizzazione, formazione;
- **quando succede qualcosa**: registrare subito violazioni e richieste degli interessati e rispettare i termini;
- **almeno una volta l'anno**: rivedere il registro e le misure di sicurezza, verificare nomine e contratti, ripetere la formazione, controllare gli amministratori di sistema, stampare il registro aggiornato con la data;
- **conservare le prove**: documenti firmati, attestati, verbali, registri.

Il programma accompagna questa routine con lo Scadenzario, il Riepilogo conformità, gli allegati e il pacchetto normativo che si aggiorna da solo. Le scelte di merito (quale base giuridica, quanto conservare, se notificare una violazione) restano del titolare, che nei casi dubbi farà bene a sentire il proprio consulente o DPO.

43. Obblighi GDPR e dove si gestiscono

Obbligo	Riferimento	Dove nel programma
Registro delle attività di trattamento	art. 30	Registro dei trattamenti › Stampa registro PDF
Liceità e basi giuridiche	artt. 6, 9, 10	Trattamento › Finalità e Interessati e dati
Informativa agli interessati	artt. 13-14	Informativa (Word)
Contratto con i responsabili	art. 28	Soggetti e nomine › Genera nomina
Accordo tra contitolari	art. 26	Soggetti e nomine › Genera nomina
Istruzioni agli autorizzati	art. 29; art. 2-quaterdecies Codice	Soggetti e nomine › lettera di autorizzazione
Amministratori di sistema	Provv. Garante 27/11/2008	Soggetti e nomine › designazione

Sicurezza del trattamento	art. 32	Trattamento › misure; Analisi dei rischi; Formazione
Violazioni: registro, notifica, comunicazione	artt. 33-34	Registro violazioni
Valutazione d'impatto	art. 35	Valutazioni d'impatto (DPIA)
Consultazione preventiva	art. 36	DPIA › Conclusioni
Designazione del DPO	artt. 37-39	Titolari del trattamento › Privacy; Soggetti e nomine
Diritti degli interessati e termini	artt. 12, 15-22	Richieste degli interessati
Trasferimenti extra UE	artt. 44-49	Trattamento › Destinatari
Responsabilizzazione (dimostrare la conformità)	art. 5.2, art. 24	Riepilogo conformità; Allegati; Scadenzario

44. Glossario

Titolare del trattamento	Chi decide perché e come trattare i dati: l'impresa, lo studio, il professionista o l'ente (art. 4, n. 7).
Responsabile del trattamento	Chi tratta i dati per conto del titolare (fornitori, consulenti).
Sub-responsabile	Il fornitore di cui si serve il responsabile.
Contitolari	Due o più soggetti che decidono insieme finalità e mezzi.
Autorizzato	La persona interna che tratta i dati secondo le istruzioni del titolare.
Interessato	La persona a cui si riferiscono i dati.
Dato personale	Qualsiasi informazione su una persona identificata o identificabile.
Categorie particolari	Dati sensibili: salute, origine etnica, opinioni politiche, religione, sindacato, dati genetici e biometrici, vita od orientamento sessuale (art. 9).
Dati giudiziari	Dati su condanne penali e reati (art. 10).
Base giuridica	La ragione che rende lecito il trattamento (art. 6).
Legittimo interesse	Un interesse concreto del titolare che prevale sui diritti delle persone.
Informativa	Il documento che spiega alle persone come sono trattati i loro dati.
Registro dei trattamenti	L'elenco documentato dei trattamenti (art. 30).
DPIA	Valutazione d'impatto sulla protezione dei dati (art. 35).
Data breach	Violazione dei dati personali (artt. 33-34).
DPO	Responsabile della protezione dei dati (artt. 37-39).
Amministratore di sistema	Chi gestisce sistemi, reti e banche dati.
Paese terzo	Paese fuori dall'Unione europea.
Rischio inerente /	Il rischio prima e dopo le misure di sicurezza.

residuo	
Garante	Il Garante per la protezione dei dati personali, autorità di controllo italiana.
EDPB	Comitato europeo per la protezione dei dati: riunisce le autorità europee e adotta linee guida comuni.
Accountability	Responsabilizzazione: il titolare deve rispettare le regole e saperlo dimostrare (artt. 5.2 e 24).
Pseudonimizzazione	Trattare i dati in modo che non si possano attribuire a una persona senza informazioni aggiuntive conservate a parte (art. 4, n. 5).
Pacchetto normativo	L'insieme di norme, termini, elenchi e testi che il programma applica; si aggiorna da solo, firmato da Korevium.