Documento di supporto alla valutazione d'impatto

Elementi che GREM S.R.L. fornisce al titolare del trattamento per la sua valutazione d'impatto sulla protezione dei dati (art. 35 GDPR), ai sensi dell'art. 28.3.f. La valutazione e le sue conclusioni restano del titolare. Versione del 21 settembre 2026.

1. Perché la valutazione è necessaria

Il trattamento riguarda dati biometrici usati per identificare in modo univoco una persona (art. 9), su larga scala, con tecnologie nuove, e condiziona l'accesso a un servizio: ricade nei criteri dell'art. 35.3 e nell'elenco del Garante dei trattamenti soggetti a valutazione d'impatto (provvedimento n. 467 dell'11 ottobre 2018).

2. Descrizione del trattamento

1. Il titolare apre una pratica e genera un link monouso, valido 30 minuti.
2. La persona legge l'informativa del titolare e dà il consenso; il sistema registra versione del testo, data, ora e indirizzo IP.
3. La persona fotografa il documento. Il servizio di lettura estrae i dati; la zona a lettura ottica e il codice fiscale sono verificati con le loro cifre di controllo.
4. Se il telefono ha l'NFC, la persona legge il chip. Il server verifica la firma dello Stato emittente e la prova anti-copia.
5. La persona fa il controllo dal vivo: una breve ripresa del volto. Il server rilegge l'esito da AWS e confronta il volto con quello del documento o del chip, ottenendo una misura di somiglianza.
6. Il nome letto viene confrontato con le liste di sanzioni, PEP e procedimenti penali.
7. Una persona esamina misure, immagini, dati letti e screening e decide: approvata, rifiutata o da rifare. Chi sia dipende dal piano (vedi sotto). Se il titolare ha attivato l'approvazione automatica, le sole pratiche verdi su tutti i controlli (chip firmato dallo Stato, prova anti-copia, documento non scaduto, controllo dal vivo e volto con valori pari o superiori alle soglie dedicate scelte dal titolare, da 90 a 100, screening senza riscontri) sono approvate senza l'esame di una persona. Nessun rifiuto è deciso dalla macchina. Ogni decisione registra chi l'ha presa, quando, le misure e le soglie in vigore.
8. Il titolare riceve la notifica dell'esito e legge il fascicolo. I dati sono cancellati alle scadenze impostate.

Piani. Nel piano **Standard** le pratiche non approvate automaticamente le decidono i proprietari e gli amministratori del titolare, dalla dashboard: valutano anche ogni riscontro dello screening, con i dati della persona in lista, e possono rieseguirlo. Il personale di GREM S.R.L. non apre né consulta queste pratiche: il software lo impedisce. Nel piano **Istituzionale** le decide un operatore di GREM S.R.L., per conto del titolare e su sua istruzione: apre la pratica, e ogni apertura è registrata; valuta i riscontri; può correggere i dati letti male. È l'unico piano in cui il personale di GREM accede ai dati identificativi per la revisione. In entrambi i piani il titolare resta titolare del trattamento e soggetto obbligato ai sensi del D.Lgs. 231/2007: decisione di instaurare il rapporto, valutazione del rischio e adeguata verifica restano sue.

I dati trattati, i destinatari, i luoghi e i tempi sono nell'Allegato A e nell'Allegato C dell'*Accordo sul trattamento dei dati* e nell'elenco dei *Sub-responsabili*.

3. Necessità e proporzionalità

- **Finalità determinata**: l'adeguata verifica imposta dal D.Lgs. 231/2007; nessun altro uso, nessun addestramento di modelli.
- **Base giuridica**: obbligo di legge per l'identificazione (art. 6.1.c); consenso esplicito per il trattamento biometrico (art. 9.2.a), con un'alternativa non biometrica che il titolare offre sui propri canali.
- **Minimizzazione**: nessun modello biometrico conservato, solo una misura numerica; allo screening va solo il nome; le notifiche automatiche non contengono dati delle persone verificate; il ruolo «membro» del titolare non vede dati né immagini.
- **Limitazione della conservazione**: fotografie 30 giorni al massimo salvo diversa scelta del titolare; dati identificativi per il termine di legge dalla fine del rapporto; pratiche non concluse cancellate dopo 12 mesi salvo diversa scelta; cancellazione automatica ogni sei ore.
- **Esattezza**: nel piano Istituzionale, correzioni solo durante la revisione di un operatore di GREM, con il valore precedente conservato e il titolare avvisato; nel piano Standard, se i dati letti sono errati, il titolare chiede alla persona di rifare la verifica.

4. Rischi e misure

Rischio per la persona	Probabilità e gravità prima delle misure	Misure	Rischio residuo
Qualcuno si fa passare per la persona con un documento falso o altrui	Media, grave	Firma dello Stato sul chip, prova anti-copia, controllo dal vivo, confronto del volto, decisione umana	Basso
Un'approvazione automatica accetta una persona che non è chi dice di essere	Bassa, grave	Solo se attivata dal titolare con istruzione registrata; solo con dati firmati dallo Stato e chip che prova di non essere una copia; soglie non inferiori a 90; screening senza riscontri; mai un rifiuto; ogni approvazione automatica è riconoscibile e riesaminabile su richiesta	Basso
Una ripresa falsa (video registrato, maschera, immagine sintetica) supera il controllo dal vivo	Media, grave	Controllo dal vivo di AWS con esito letto dal server e legato alla pratica; soglia di confidenza; decisione umana	Basso-medio
La persona viene respinta per un errore della macchina, anche in modo discriminatorio	Media, media	Nessun rifiuto automatico; chi decide vede le misure e le immagini; possibilità di rifare; alternativa non biometrica	Basso
Furto o divulgazione delle immagini del volto e del documento	Bassa, molto grave	Immagini fuori dal database, cifrate, accessibili solo con link di 5 minuti; conservazione breve; accessi del personale registrati	Basso
Uso dei dati per altri scopi o per addestrare modelli	Bassa, grave	Divieto contrattuale per noi e per i sub-responsabili	Basso
Conservazione oltre il necessario	Media, media	Cancellazione automatica; date fissate e non ricalcolabili; cancellazione della singola pratica	Basso

Rischio per la persona	Probabilità e gravità prima delle misure	Misure	Rischio residuo
Omonimia con una persona sanzionata porta a un rifiuto ingiusto	Media, grave	Ogni riscontro è valutato da una persona prima della decisione (del titolare nel piano Standard, un operatore di GREM nel piano Istituzionale), confrontando i dati della persona in lista; motivo registrato	Basso
Accesso non autorizzato di un dipendente del fornitore	Bassa, grave	Nel piano Standard il personale del fornitore non può aprire le pratiche; nel piano Istituzionale ruoli separati, registro inalterabile di ogni accesso, vincoli di riservatezza	Basso
Accesso improprio da parte del personale del titolare, che nel piano Standard vede immagini e dati per decidere	Bassa, grave	Decidono solo proprietari e amministratori; il ruolo «membro» non vede dati né immagini; immagini solo tramite link di 5 minuti; ogni decisione registra chi l'ha presa; **ogni apertura di una pratica dal pannello è registrata** con persona, data e indirizzo, e il registro esce nell'esportazione dell'organizzazione (`registro.jsonl`); verifica in due passaggi disponibile per il personale del titolare	Da valutare dal titolare, secondo le proprie misure interne
Esclusione di chi non ha uno smartphone adatto	Media, media	La lettura del chip è facoltativa; alternativa offerta dal titolare	Basso

5. Cosa deve aggiungere il titolare

- La propria valutazione del rischio, la classificazione della funzione e le alternative che offre.
- Il parere del proprio responsabile della protezione dei dati, se nominato.
- Eventualmente, il parere degli interessati o dei loro rappresentanti (art. 35.9).
- La decisione sulla consultazione preventiva del Garante, se il rischio residuo resta elevato (art. 36).
- Nel piano Standard: chi del proprio personale decide le pratiche, come è formato a leggere misure e riscontri dello screening e come ne controlla gli accessi.
- Se attiva l'approvazione automatica: la valutazione del rischio residuo di un'approvazione senza l'esame di una persona, l'informazione agli interessati e il modo in cui risponde alle richieste di intervento umano (art. 22, par. 3).