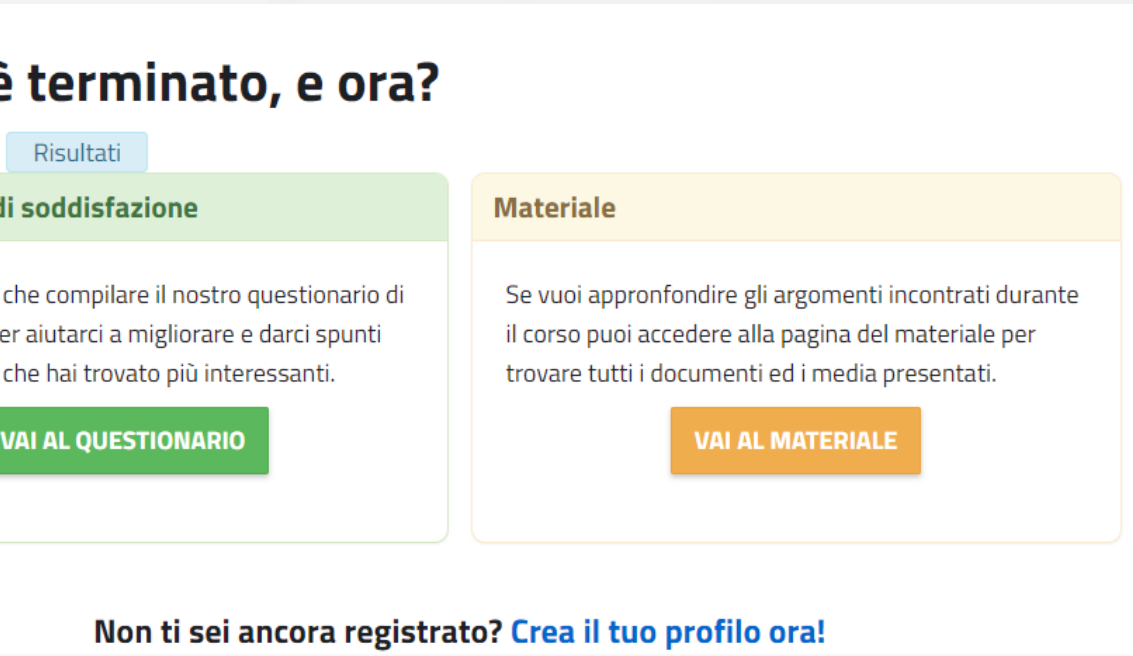
SI.NET
Servizi Informatici

La protezione dei dati a 6 mesi dal GDPR

Questionario di soddisfazione dell'utenza

http://sinet.herald.cloud/questionario

(Ricorda: il sistema ti chiederà di eseguire il login, se non lo hai già fatto prima di scaricare il materiale o compilare il questionario effettua la registrazione)



Contenuti

9:30 - 9:45	**IL CONCETTO DI PRIVACY E LA NUOVA NORMATIVA PER LA PROTEZIONE DEI DATI** Paolo Tiberi
9:45 - 10:30	**ALBO ON LINE E NORMATIVA PRIVACY** Luigi Cristiano
10:30 – 11:00	**LE PROCEDURE DI DATA BREACH E DPIA** Paolo Tiberi
11:00 - 11:30	*Coffee break*
11:30 - 13:00	**RISCHI E INCIDENTI** Aldo Lupi

Direttiva 95/46/CE

- Legge 675/1996
- DPR 318/1999 «misure minime di sicurezza»

Codice privacy
d.lgs 196/03
(e allegati)

Provvedimento del garante della privacy -
27/11/2008 (amministratori di sistema)
DL 9/2/2012 n.5 (soppressione DPS) -

- **Direttiva UE 680/2016 Tutela «privacy» in ambito di prevenzione, contrasto e repressione crimini**
- **Direttiva UE 1148/2016 NIS Sicurezza reti e sistemi informativi**

Regolamento UE 679/2016

Il Regolamento UE 679/16 e l'Italia

- Che ne è del Codice privacy?
  - Il regolamento UE è immediatamente applicabile negli stati membri senza bisogno di leggi particolari che ne recepiscano la normatività
  - In molti stati membri sono state emanate norme particolari (Germania - BDSG)

In Italia?

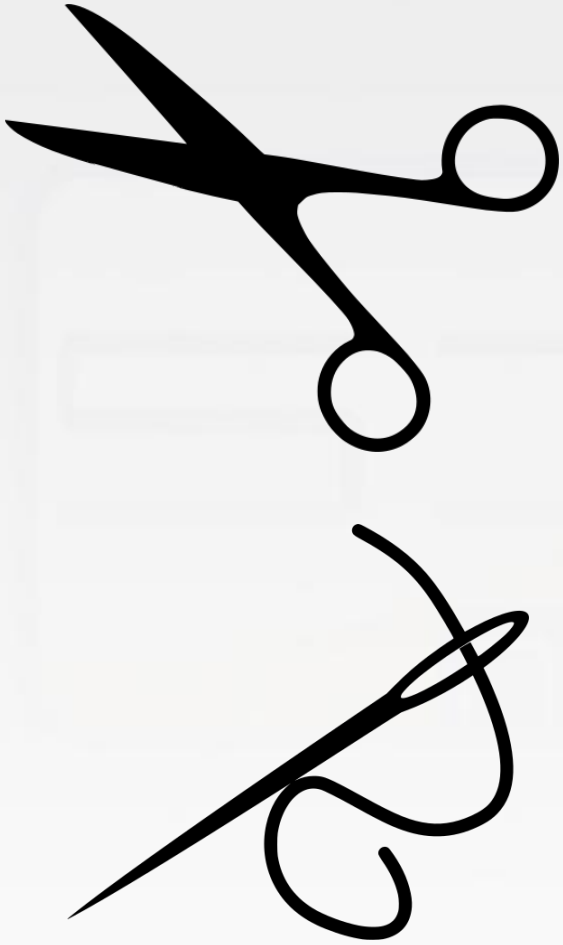
INTERAZIONI NORMATIVE

Regolamento UE 2016/679

D.Lgs. 196/2003

Come rivisto dal d.lgs 101/2018

IL «TAGLIA E CUCI» DEL D.LGS. 101/18



Abrogazione degli articoli non conformi al Regolamento UE

Rimando al Regolamento UE

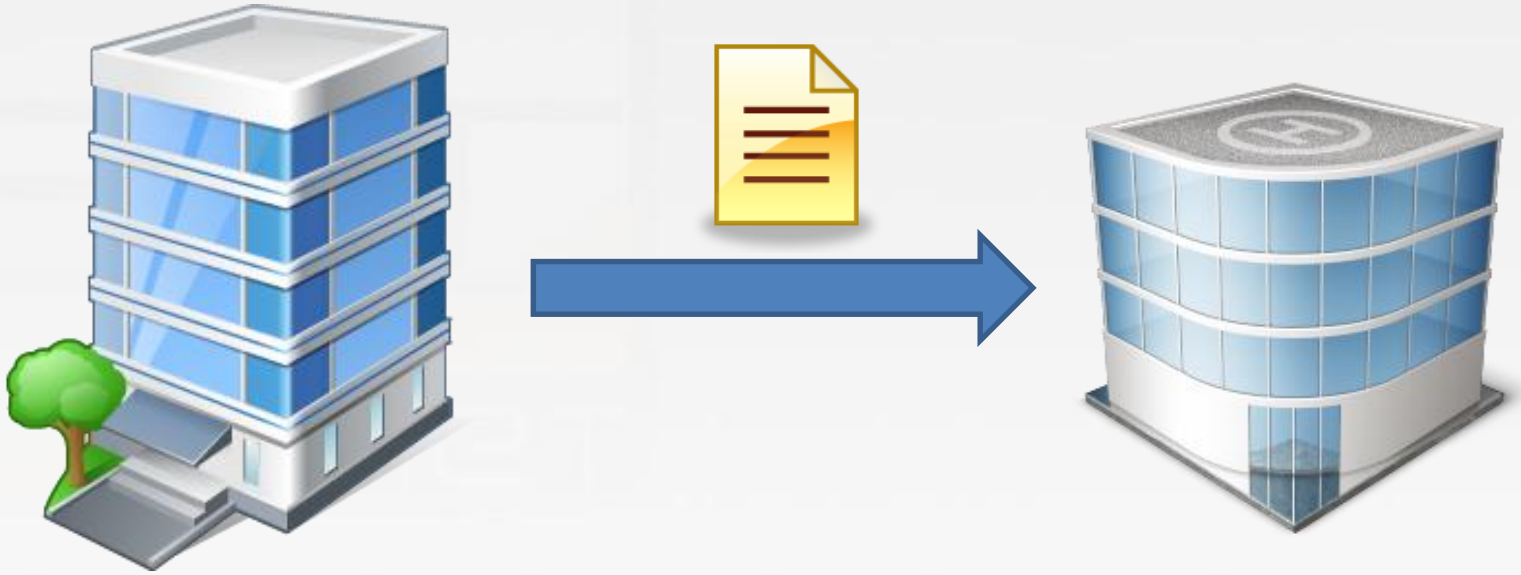
I TRATTAMENTI DELLE PA

	Artt. 18 - 22	Abrogati
	Art. 2-ter	Base giuridica per il trattamento di dati personali effettuato per l'**esecuzione di un compito di interesse pubblico** o connesso all'esercizio di pubblici poteri
	Art. 2-sexies	Trattamento di **categorie particolari di dati** personali necessario per motivi di **interesse pubblico rilevante**
	Art. 2-septies	Misure di garanzia per il trattamento dei **dati genetici, biometrici e relativi alla salute**
	Art. 2-octies	Principi relativi al trattamento di **dati relativi a condanne penali e reati**

COMUNICAZIONE TRA TITOLARI (3)

Art 2-ter par 3

*Comunicazione di dati **non** particolari o giudiziari a soggetti che intendono trattarli per altre finalità*

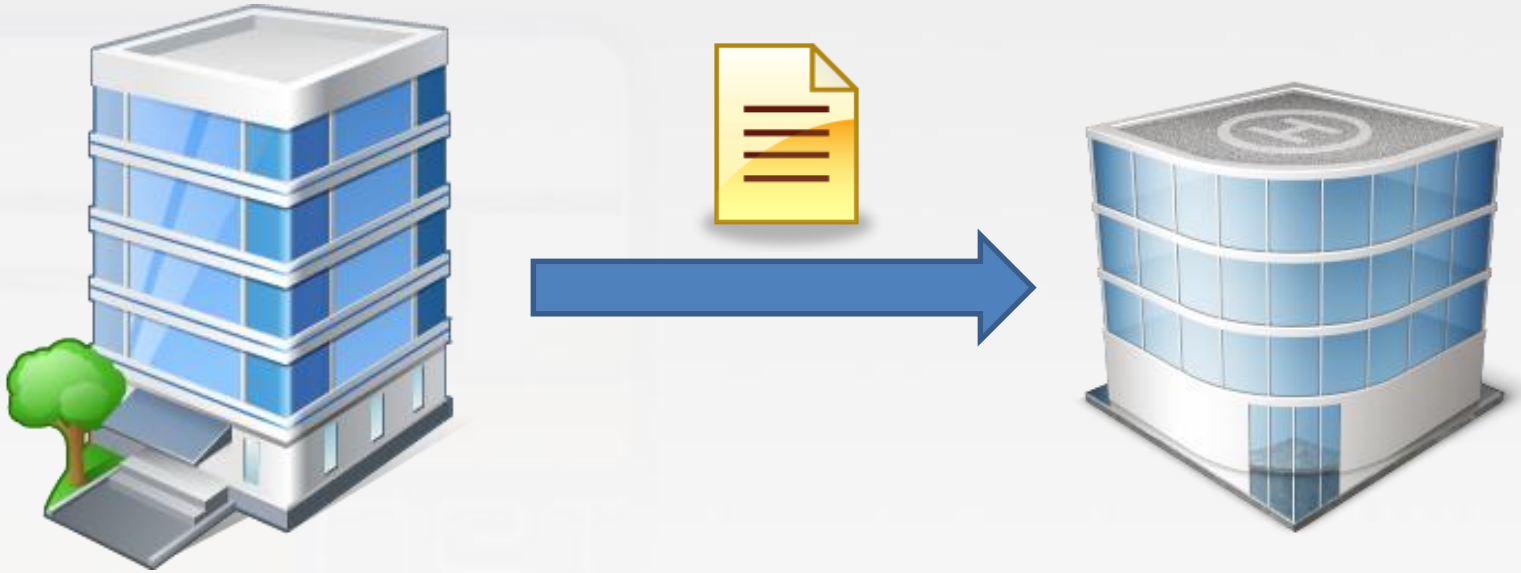


AMMESSA se prevista da norma di legge o regolamento.

COMUNICAZIONE TRA TITOLARI (1)

Art 2-ter par 2

Comunicazione tra titolari di dati non particolari o giudiziari



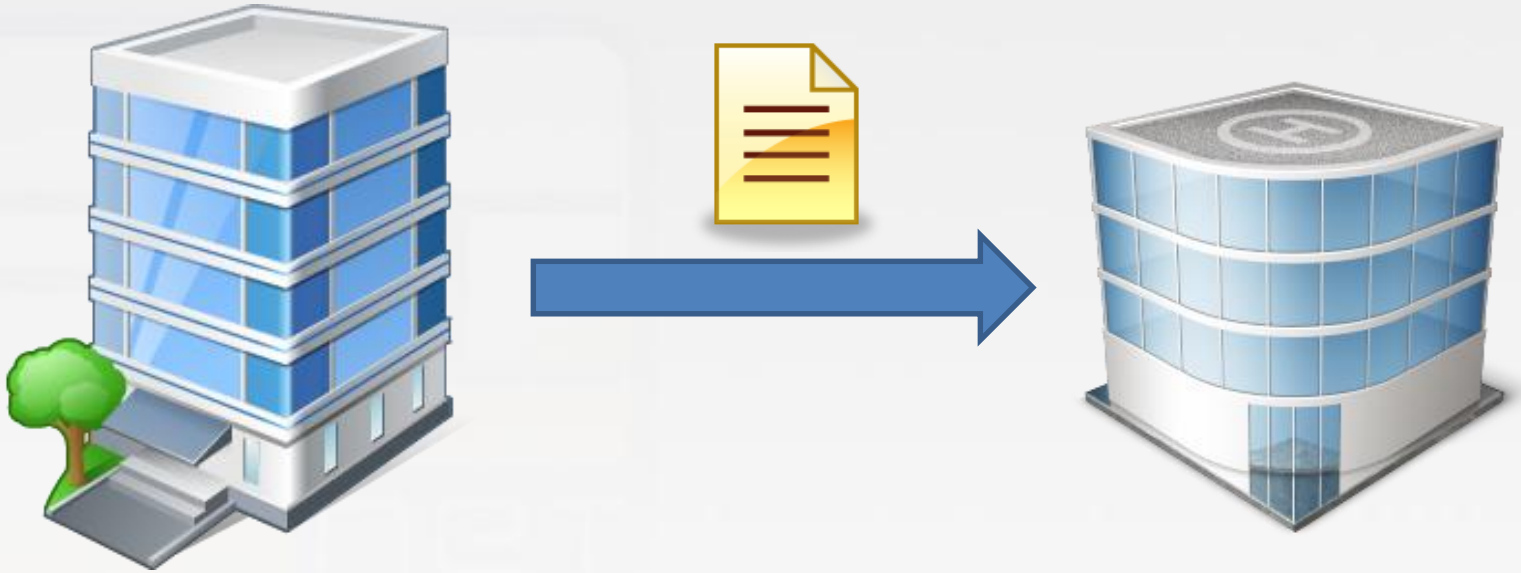
Per l'esecuzione di un interesse pubblico o connesso all'esercizio di pubblici poteri AMMESSA se prevista da norma di legge o regolamento.

OPPURE….

COMUNICAZIONE TRA TITOLARI (2)

Art 2-ter par 2

Comunicazione tra titolari di dati non particolari o giudiziari

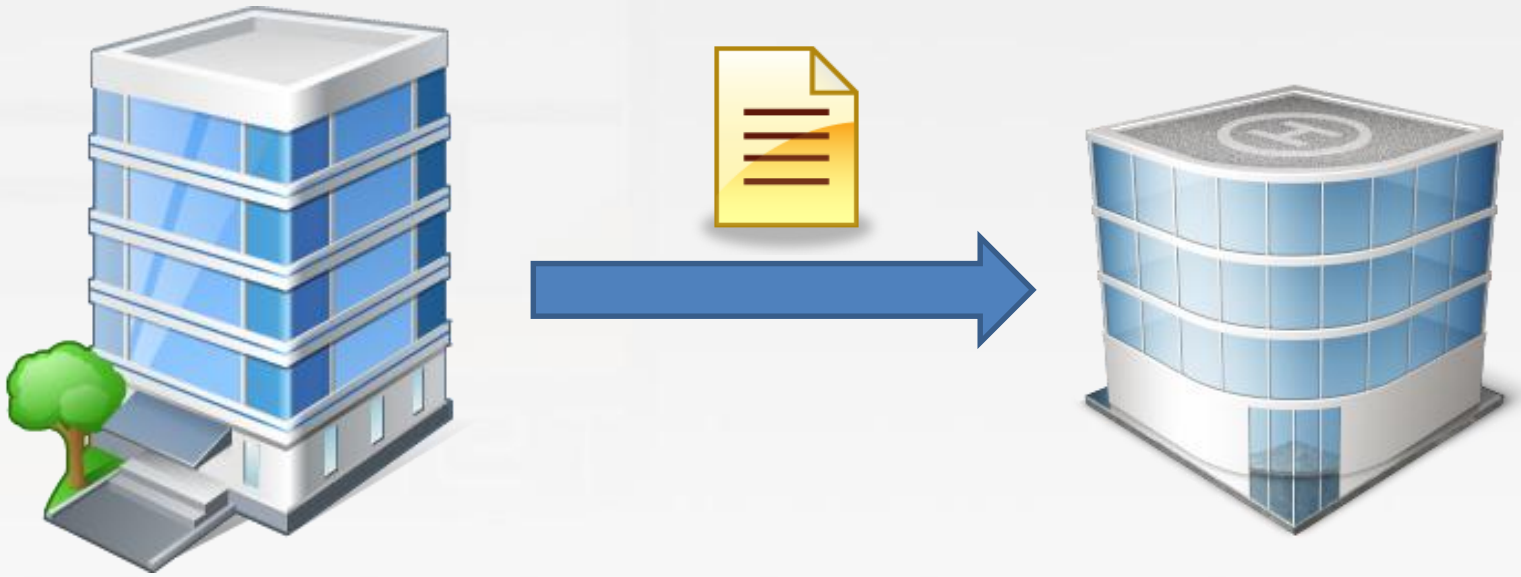


Per l'esecuzione di un interesse pubblico o connesso all'esercizio di pubblici poteri AMMESSA quando necessaria per lo svolgimento di funzioni istituzionali**, dopo 45 giorni dalla relativa comunicazione al Garante** (senza che abbia espresso diniego o fornito prescrizioni).

COMUNICAZIONE TRA TITOLARI (3)

Art 2-ter par 3

Comunicazione di dati non particolari o giudiziari a soggetti che intendono trattarli per altre finalità



AMMESSA se prevista da norma di legge o regolamento.

DIFFUSIONE

Art 2-ter par 3

Diffusione di dati non particolari o giudiziari

«DIFFUSIONE» → il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (Art 2-ter par 4)

AMMESSA se prevista da norma di legge o regolamento.

CATEGORIE PARTICOLARI DI DATI

Art 2-sexies

Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante

AMMESSO se

- previsto da norma di legge o regolamento;
- sono specificati i tipi di dati che possono essere trattati;
- sono esplicitate le operazioni eseguibili;
- è esplicito il motivo di interesse pubblico rilevante;
- sono definite le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Il par. 2 definisce gli ambiti di rilevante interesse pubblico.

DATI GENETICI, BIOMETRICI RELATIVI ALLA SALUTE

Art. 2-septies

Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute

AMMESSO

In conformità delle misure di garanzia disposte dal Garante della Privacy, con provvedimento adottato con cadenza almeno biennale

TALI DATI NON POSSONO ESSERE DIFFUSI

DATI RELATIVI A CONDANNE PENALI E REATI

Art. 2-octies

Principi relativi al trattamento di dati relativi a condanne penali e reati

…fatto salvo quanto previsto dal D.Lgs,18 maggio 2018, n. 51 (rimando a Decreto del Ministero della Giustizia)

AMMESSO

se previsto da norma di legge o regolamento che prevedano garanzie appropriate per i diritti e le libertà degli interessati.

Previsti al par. 3 diversi contesti per cui è consentito il trattamento di dati giudiziari.

TITOLARI, RESPONSABILI, INCARICATI

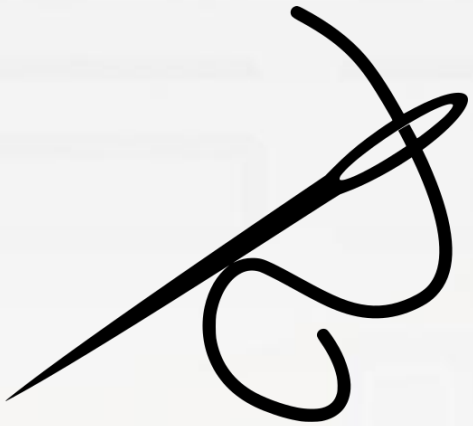
D.Lgs. 196/2003

ABROGAZIONE

Art. 4 (definizioni)

Titolo IV (soggetti che effettuano il trattamento)

TITOLARI, RESPONSABILI, INCARICATI



Regolamento UE 2016/679

Art. 4 (definizioni)

Artt. 28, 29 (responsabile del trattamento)

AUTORIZZATI AL TRATTAMENTO

Art. 2-quaterdecies

Attribuzione di funzioni e compiti a soggetti designati

1. **Il titolare** o il responsabile del trattamento **possono prevedere**, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che **specifici compiti e funzioni connessi al trattamento di dati personali** siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.
2. Il titolare o il responsabile del trattamento individuano **le modalità più opportune per autorizzare al trattamento** dei dati personali le persone che operano sotto la propria autorità diretta.

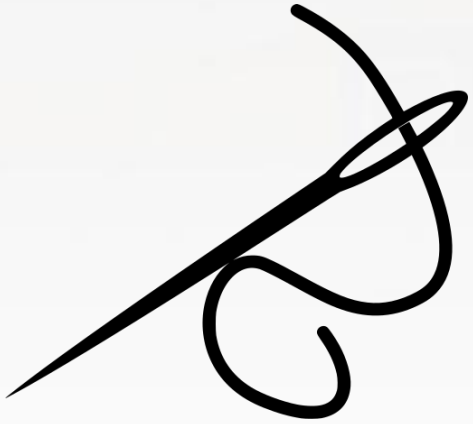
TRATTAMENTI CHE PRESENTANO RISCHI ELEVATI

Art. 2-quinquiesdecies

Trattamento che presenta rischi elevati per l'esecuzione di un compito di interesse pubblico

Nei **trattamenti** svolti per l'esecuzione di un compito di interesse pubblico che possono presentare **rischi elevati, il Garante delle Privacy può prescrivere misure e accorgimenti a garanzia dell'interessato**, che il titolare del trattamento è tenuto ad adottare (richiamo art. 35 Regolamento UE 2016/679).

D.Lgs. 196/2003
ABROGAZIONE
Titolo III (Regole generali per il trattamento dei dati)



Regolamento UE 2016/679
Artt. 13 e 14

INFORMATIVE

DICITURE CORRETTE

- ai sensi del Reg. UE 2016/679 e del D.Lgs. 196/2003
- ai sensi del Reg. UE 2016/679 e D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018
- ai sensi dell’art. 13 del Reg. UE 2016/679

DICITURA SCORRETTA

- ai sensi dell’art. 13 del D.Lgs. 196/2003

Violazione dati personali

Articolo 33

Notifica di una violazione dei dati personali all'autorità di controllo (C85, C87, C88)

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 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. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Il titolare del trattamento dovrà comunicare eventuali violazioni dei dati personali (*data breach*) all'Autorità nazionale di protezione dei dati.
Se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare le possibili conseguenze negative.

GDPR – violazione dati personali

SI.NET Servizi Informatici

COSA CAMBIA

- A partire dal 25 maggio 2018, **tutti i titolari** – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno notificare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, **entro 72 ore** e comunque "senza ingiustificato ritardo", ma **soltanto se ritengono probabile che da tale violazione derivino rischi** per i diritti e le libertà degli interessati (si veda considerando 85). Pertanto, **la notifica all'Autorità** dell'avvenuta violazione **non è obbligatoria**, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34, che coincidono solo in parte con quelle attualmente menzionate nell'art. 32-bis del Codice. **I contenuti della notifica** all'Autorità e della comunicazione agli interessati sono indicati, **in via non esclusiva, agli art. 33 e 34 del regolamento**.

Raccomandazioni

Tutti i titolari di trattamento dovranno in ogni caso **documentare le violazioni** di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (si veda art. 33, paragrafo 5); tale obbligo non è diverso, nella sostanza, da quello attualmente previsto dall'art. 32-bis, comma 7, del Codice.
Si raccomanda, pertanto, ai titolari di trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

DATA BREACH: LA TIPOLOGIE

1- Distruzione dei dati (violazione della disponibilità del dato)

2- Perdita di credenziali di accesso (violazione della disponibilità e della riservatezza)

3- Modifica del dato (violazione della correttezza del dato)

4- Divulgazione non autorizzata (violazione della riservatezza)

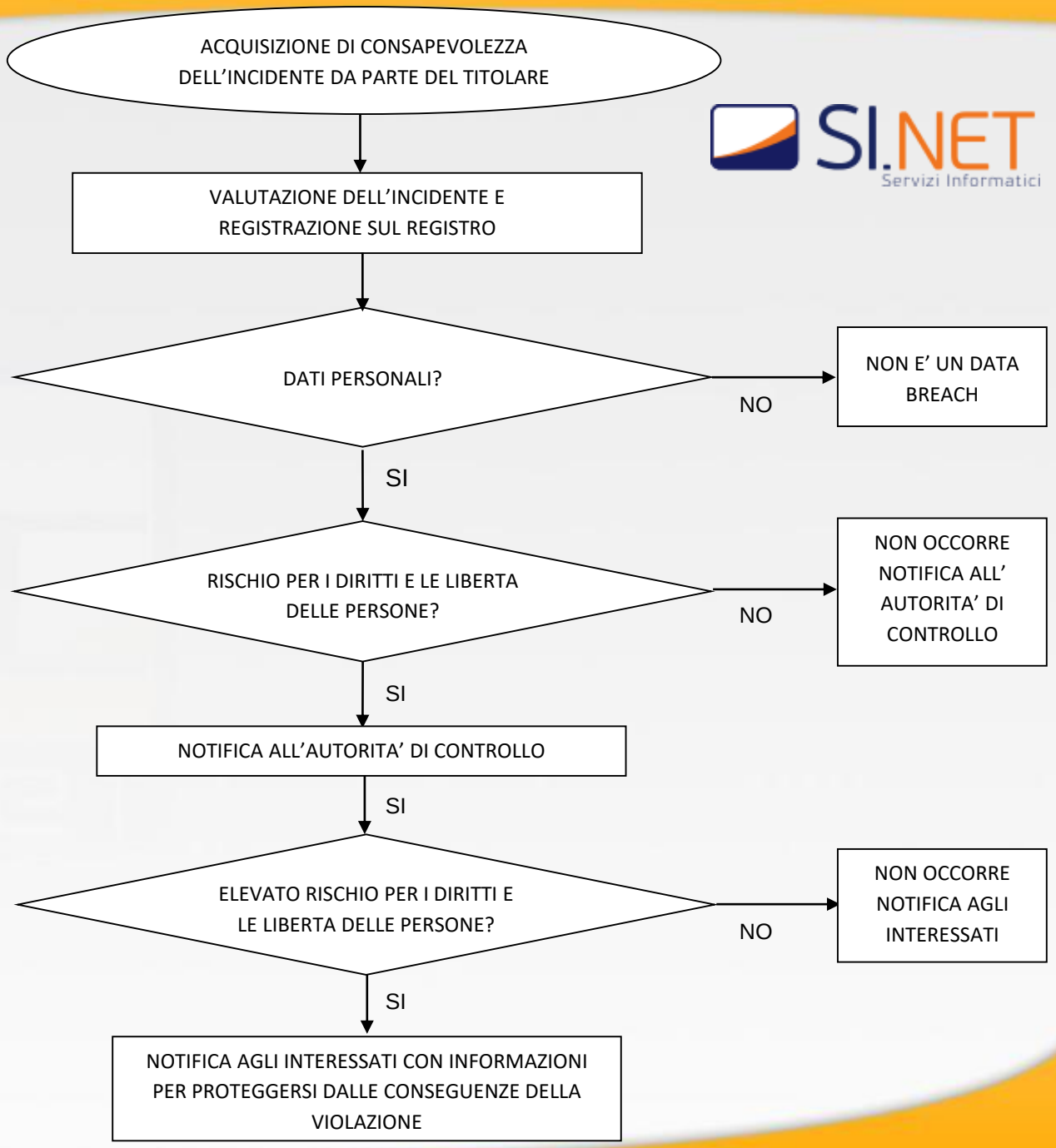
…

DATA BREACH: LA PROCEDURA

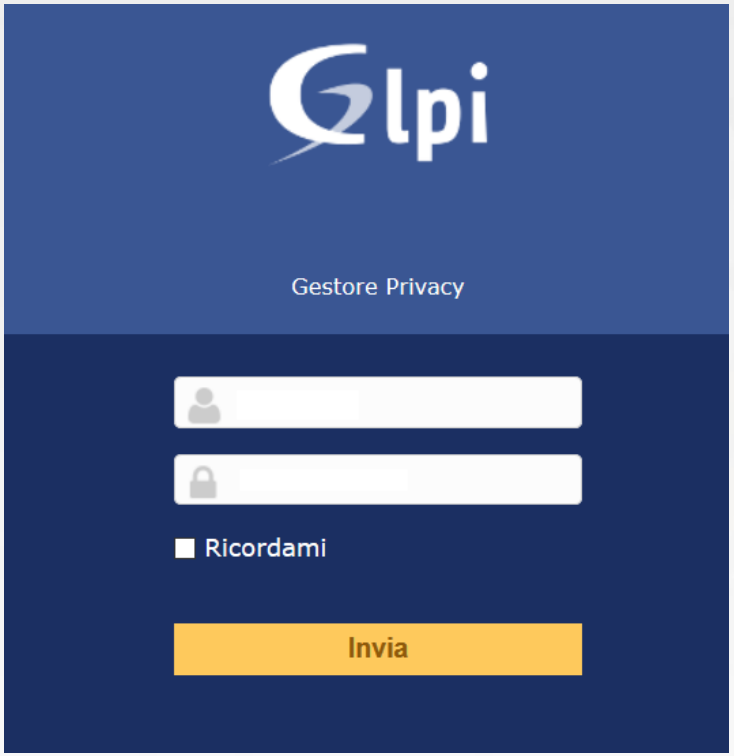
La procedura redatta da SINET:

Data breach response plan 1.3:

https://www.sinetinformatica.it/atti-di-approvazione-ed-adozione-documenti-relativi-alla-protezione-dei-dati-personali/



DATA BREACH: LA PROCEDURA (1)



1. Collegarsi all'indirizzo https://privacy.sinetinformatica.it/ utilizzando le credenziali rilasciate
2. Collegarsi ed cliccare sul link "Inserisci una chiamata"
3. Aprire una chiamata di tipo "Incidente" – Categoria "Incident" e segnalare l'accaduto, eventualmente allegando dei files che possano contribuire a chiarire l'incidente:
4. Valutare insieme al Responsabile per la Protezione dei Dati la portata dell'incidente, la gravità e le azioni da intraprendere seguendo il processo indicato al paragrafo 6.
5. Procedere, in caso di necessità, alla segnalazione dell'eventuale violazione di sicurezza, alle notifiche necessarie con il supporto del Responsabile per la Protezione dei Dati.

Privacy Impact Assessment

Di cosa si tratta?

Una valutazione d'impatto sulla protezione dei dati è un **PROCESSO** teso a:

- **Descrivere** il trattamento;
- Valutarne la **necessità e la proporzionalità;**
- Contribuire a **gestire i rischi** per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando tali rischi e determinando le misure per affrontarli.

Una valutazione di impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità al GDPR

DPIA nel GDPR

Considerando n.(89)

La direttiva 95/46/CE ha introdotto un obbligo generale di notificare il trattamento dei dati

- La notificazione comporta oneri amministrativi e finanziari e non ha contribuito a migliorare la protezione dei dati personali.

È pertanto opportuno abolire tali obblighi generali e indiscriminati di notifica

- **sostituirli con meccanismi e procedure efficaci** che si concentrino piuttosto su quei tipi di trattamenti che potenzialmente presentano **un rischio elevato** per i diritti e le libertà delle persone fisiche, per loro natura, ambito di applicazione, contesto e finalità

DPIA nel GDPR

Considerando n.(89) **– trattamenti per i quali è obbligatoria la DPIA**

…

Tra i trattamenti sono inclusi:

- Trattamenti che comportano l'utilizzo di **nuove tecnologie**
- Trattamenti in relazione ai quali il titolare **non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati**
- Trattamenti per i quali la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del **tempo trascorso dal trattamento iniziale**.

DPIA nel GDPR

Articolo 35 GDPR (*comma 3)*

3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

   a) una **valutazione sistematica e globale di aspetti personali relativi a persone fisiche**, basata su un trattamento automatizzato, compresa la **profilazione**, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

   b) il **trattamento, su larga scala, di categorie particolari di dati** personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o

   c) la **sorveglianza sistematica su larga scala** di una zona accessibile al pubblico.

DPIA nel GDPR

Articolo 35 GDPR

4. L'**autorità di controllo** redige e rende pubblico un **elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto*** sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.
5. L'**autorità di controllo** può inoltre redigere e rendere pubblico **un elenco delle tipologie di trattamenti per le quali non è richiesta** una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.

*DPIA obbligatoria per…

Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 [9058979]

ALLEGATO 1 AL PROVVEDIMENTO N. 467 DELL'11 OTTOBRE 2018 [doc. web n. 9058979] (Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018)

https://www.garanteprivacy.it/documents/10160/0/ALLEGATO+1+Elenco+delle+tipologie+di+trattamenti+soggetti+al+meccanismo+di+coerenza+da+sottoporre+a+valutazione+di+impatto

DPIA nel GDPR

Articolo 35 GDPR: le deroghe

10. Qualora:

1. il **trattamento** effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e) (obbligo legale, trattamento per interesse pubblico), **trovi nel diritto dell'Unione o nel diritto dello Stato membro** cui il titolare del trattamento è soggetto una **base giuridica**,
2. tale **diritto disciplini il trattamento** specifico o l'insieme di trattamenti in questione,
3. **sia già stata effettuata una valutazione d'impatto** sulla protezione dei dati nell'ambito di una valutazione d'impatto **generale** nel contesto dell'adozione di tale base giuridica,

DPIA nel GDPR

Articolo 35 GDPR

11. Se necessario, il **titolare del trattamento procede a un riesame** per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento

Rischio elevato: criteri

1. Trattamenti valutativi o di scoring

2. Decisioni automatizzate che producono significativi effetti

3. Monitoraggio sistematico

4. Dati sensibili o dati di natura estremamente personale

Rischio elevato: criteri

5. Trattamenti di dati su larga scala

a) numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento;

b) volume dei dati oggetto di trattamento;

c) durata, o persistenza, dell'attività di trattamento;

d) ambito geografico dell'attività di trattamento

6. Combinazione o raffronto di insiemi di dati

7. Dati relativi a interessati vulnerabili

8. Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative

9. Asimmetrie e difficolta nell'esercizio dei diritti

Rischio elevato: esempi

DPIA necessaria

Utilizzo di un **sistema di telecamere** per monitorare il comportamento di guida sulle strade

- Monitoraggio sistematico
- Uso innovativo o applicazione di soluzioni tecnologiche od organizzative

---

Introduzione, su base comunale, di una **applicazione che richieda la geolocalizzazione**

- Dati aventi estremamente personale.
- Utilizzo di nuove tecnologie

Un'azienda che **monitora sistematicamente le attività dei suoi dipendenti**, controllando anche la postazione di lavoro dei dipendenti, le loro attività in Internet, ecc.

- Monitoraggio sistematico.
- Dati riguardanti soggetti interessati vulnerabili.

Rischi residui elevati

Articolo 36 GDPR (Consultazione preventiva)

1. Il **titolare** del trattamento**, prima di procedere al trattamento, consulta l'autorità** di controllo **qualora** la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il **trattamento presenterebbe un rischio elevato** in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

Rischi residui elevati

Articolo 36 GDPR

2. Qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, **l'autorità di controllo fornisce, entro** un termine di **otto settimane** dal ricevimento della richiesta di consultazione, **un parere** scritto al titolare del trattamento. Tale periodo può essere **prorogato di sei settimane**, tenendo conto della complessità del trattamento previsto. L'autorità di controllo **informa il titolare** del trattamento di tale **proroga**, unitamente ai **motivi del ritardo, entro un mese** dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.

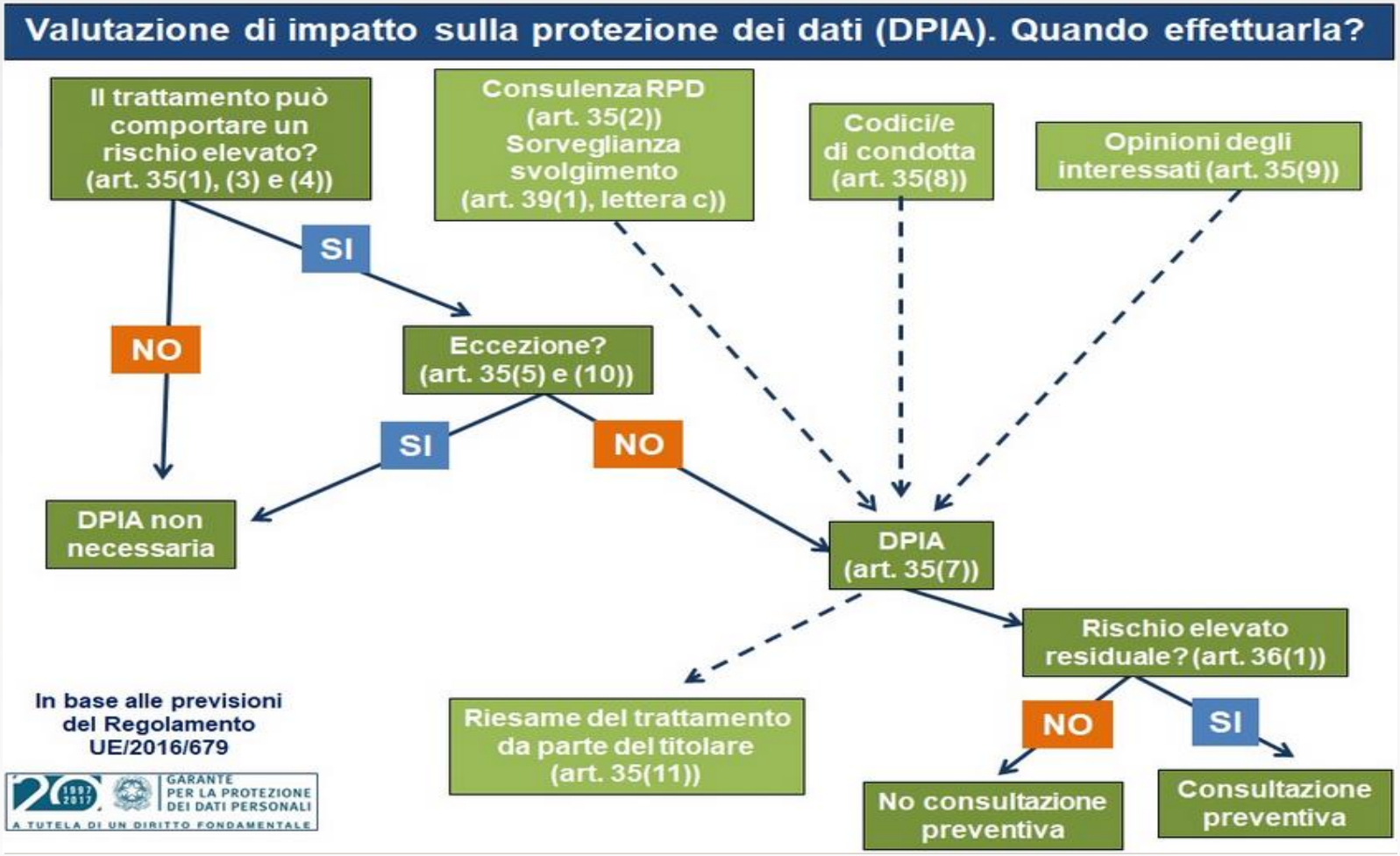
Le conseguenze delle inadempienze

(a) La mancata esecuzione di una DPIA nei casi in cui è necessaria (articolo 35, paragrafi 1, 3 e 4), (b) l'esecuzione in maniera errata di tale valutazione (articolo 35, pgf. 2 e da 7 a 9) o (c) la mancata consultazione dell'autorità di controllo laddove richiesto (articolo 36, paragrafo 3, lettera e),

POSSONO COMPORTARE una sanzione amministrativa pecuniaria pari

- a un importo massimo di **10 milioni di EUR**
- oppure, nel caso di un'impresa, pari a fino al **2% del fatturato annuo globale** dell'anno precedente, a seconda di quale importo sia superiore.

Il processo di DPIA



DPIA – Lo strumento

https://www.garanteprivacy.it/regolamentoue/DPIA

STRUMENTI

Un software per la valutazione di impatto

La **CNIL**, l´Autorità francese per la protezione dei dati, ha messo a disposizione un software di ausilio ai titolari in vista della effettuazione della **valutazione d´impatto sulla protezione dei dati (DPIA)**.

Il software - gratuito e liberamente scaricabile dal sito www.cnil.fr (**https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil**) - offre un percorso guidato alla realizzazione della DPIA, secondo una sequenza conforme alle indicazioni fornite dal WP29 nelle Linee-guida sulla DPIA.

La **versione in lingua italiana** è stata messa a punto anche con la collaborazione del Garante per la protezione dei dati personali.

Occorre sottolineare che il software è in continua evoluzione, con revisioni introdotte anche sulla base dell´esperienza raccolta e delle segnalazioni degli utenti.

Version portable

Cette version se télécharge directement sur votre poste de travail et se lance sans installation.

Disponible pour les systèmes d'exploitation suivants :

- Windows (32 et 64 bits)
- Linux (32 bits)
- Linux (64 bits)
- Mac OS

Version web

Cette version se déploie sur les serveurs de votre entreprise. Elle est disponible en mode front end ou en mode back end.

- mode front end
- mode back end

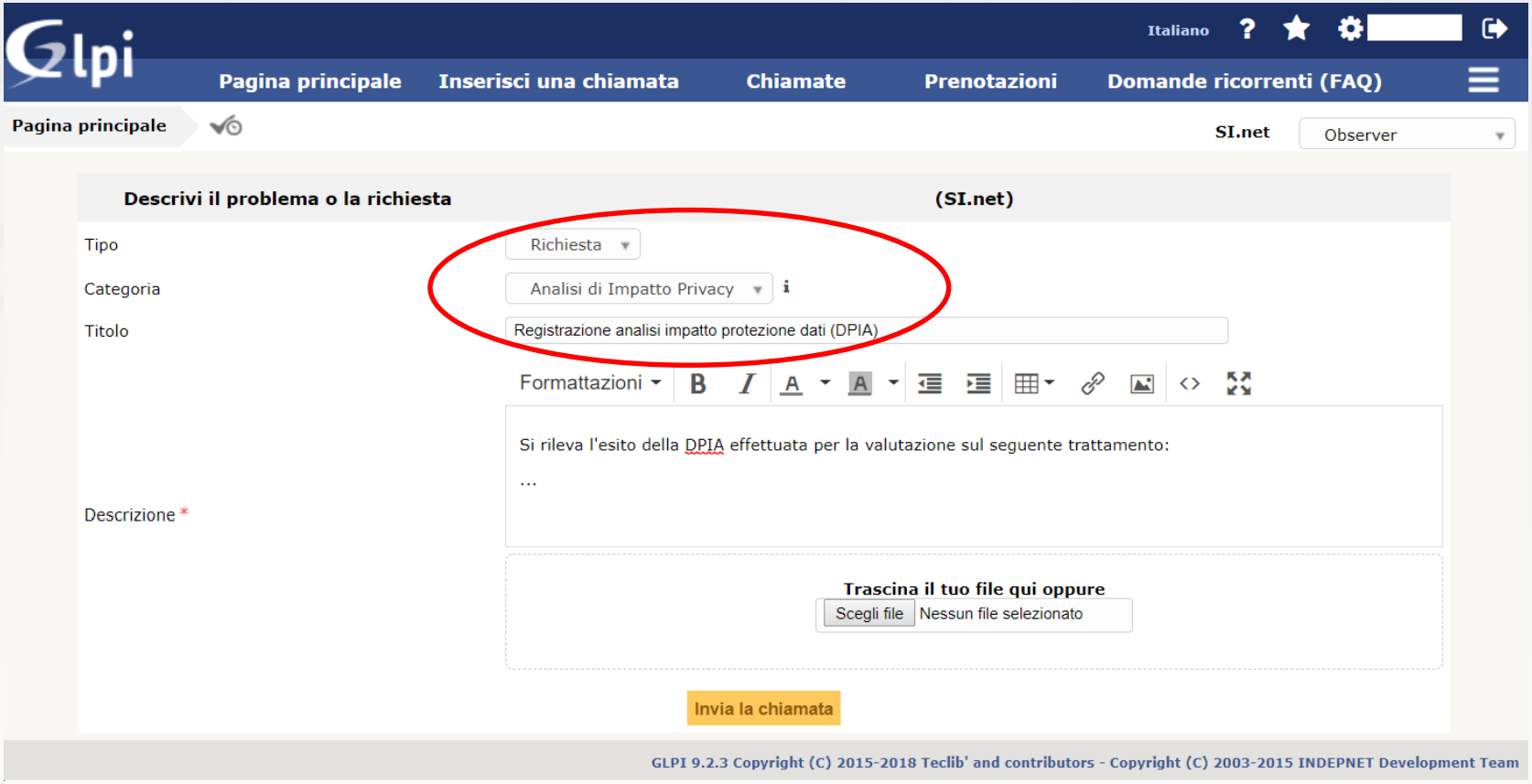
Le code étant ouvert, il est possible de l'adapter à l'écosystème informatique existant au sein de l'entreprise et de l'intégrer aux autres outils utilisés en interne.

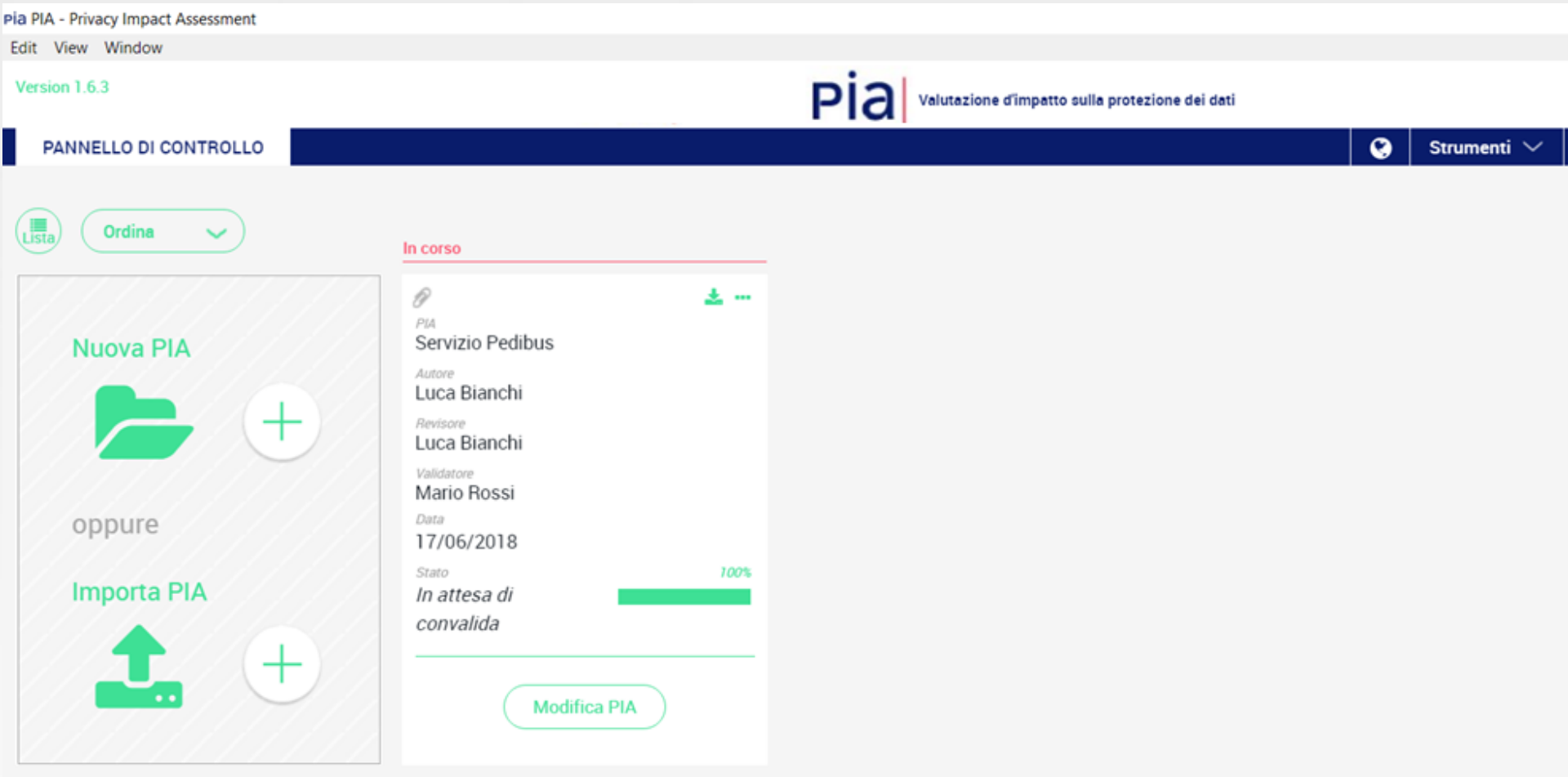
Premiers pas avec le logiciel PIA

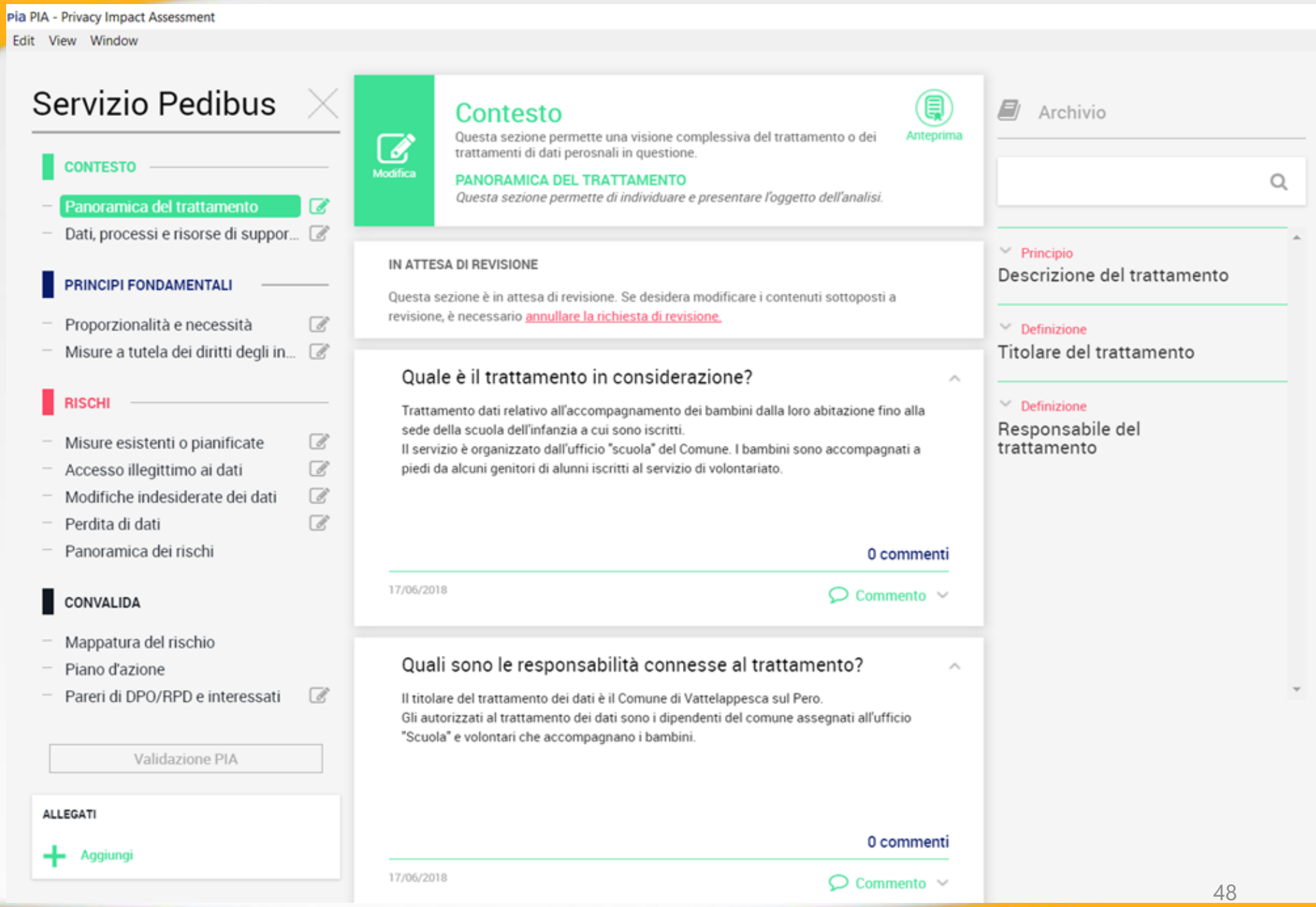
TUTORIEL | Utiliser le logiciel PIA pour mener une étude d'impact sur la protection des données

DPIA – Lo strumento

DPIA – La segnalazione a SINET




pia PIA - Privacy Impact Assessment
Edit View Window
Version 1.6.3
pia
Valutazione d'impatto sulla protezione dei dati
PANNELLO DI CONTROLLO
Strumenti
Lista
Ordina
In corso
Nuova PIA
oppure
Importa PIA
PIA
Servizio Pedibus
Autore
Luca Bianchi
Revisore
Luca Bianchi
Validatore
Mario Rossi
Data
17/06/2018
Stato
100%
In attesa di convalida
Modifica PIA


Pia PIA - Privacy Impact Assessment
Edit View Window
Servizio Pedibus
CONTESTO
Panoramica del trattamento
Dati, processi e risorse di suppor...
PRINCIPI FONDAMENTALI
Proporzionalità e necessità
Misure a tutela dei diritti degli in...
RISCHI
Misure esistenti o pianificate
Accesso illegittimo ai dati
Modifiche indesiderate dei dati
Perdita di dati
Panoramica dei rischi
CONVALIDA
Mappatura del rischio
Piano d'azione
Pareri di DPO/RPD e interessati
Validazione PIA
ALLEGATI
Aggiungi
Modifica
Contesto
Questa sezione permette una visione complessiva del trattamento o dei trattamenti di dati perosnali in questione.
PANORAMICA DEL TRATTAMENTO
Questa sezione permette di individuare e presentare l'oggetto dell'analisi.
Anteprima
IN ATTESA DI REVISIONE
Questa sezione è in attesa di revisione. Se desidera modificare i contenuti sottoposti a revisione, è necessario annullare la richiesta di revisione.
Quale è il trattamento in considerazione?
Trattamento dati relativo all'accompagnamento dei bambini dalla loro abitazione fino alla sede della scuola dell'infanzia a cui sono iscritti.
Il servizio è organizzato dall'ufficio "scuola" del Comune. I bambini sono accompagnati a piedi da alcuni genitori di alunni iscritti al servizio di volontariato.
0 commenti
17/06/2018
Commento
Quali sono le responsabilità connesse al trattamento?
Il titolare del trattamento dei dati è il Comune di Vattelappesca sul Pero.
Gli autorizzati al trattamento dei dati sono i dipendenti del comune assegnati all'ufficio "Scuola" e volontari che accompagnano i bambini.
0 commenti
17/06/2018
Commento
Archivio
Principio
Descrizione del trattamento
Definizione
Titolare del trattamento
Definizione
Responsabile del trattamento

pia PIA - Privacy Impact Assessment

Edit View Window

Servizio Pedibus

CONTESTO

- Panoramica del trattamento
- Dati, processi e risorse di suppor...

PRINCIPI FONDAMENTALI

- Proporzionalità e necessità
- Misure a tutela dei diritti degli in...

RISCHI

- Misure esistenti o pianificate
- Accesso illegittimo ai dati
- Modifiche indesiderate dei dati
- Perdita di dati
- Panoramica dei rischi

CONVALIDA

- Mappatura del rischio
- Piano d'azione
- Pareri di DPO/RPD e interessati

Validazione PIA

ALLEGATI

Flow chart Pedibus.pptx

Aggiungi

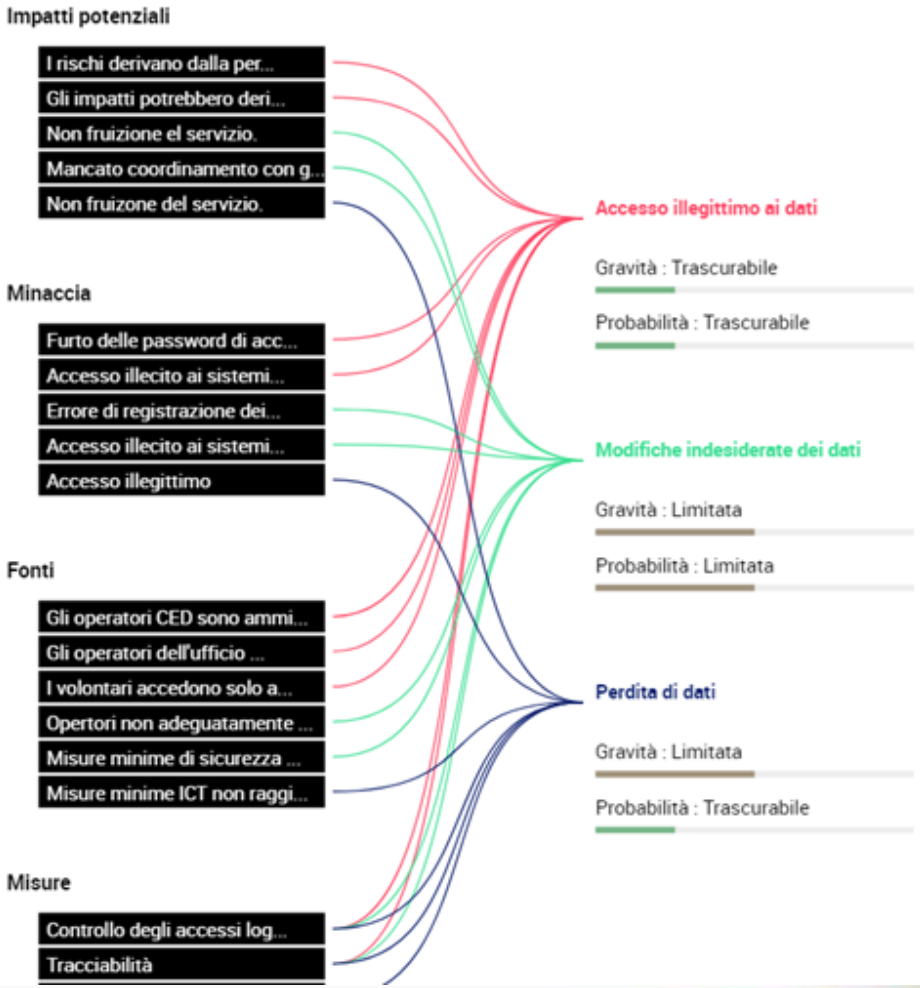
Rischi

Anteprima

Questa sezione permette di valutare i rischi per la riservatezza, alla luce delle misure esistenti o pianificate.

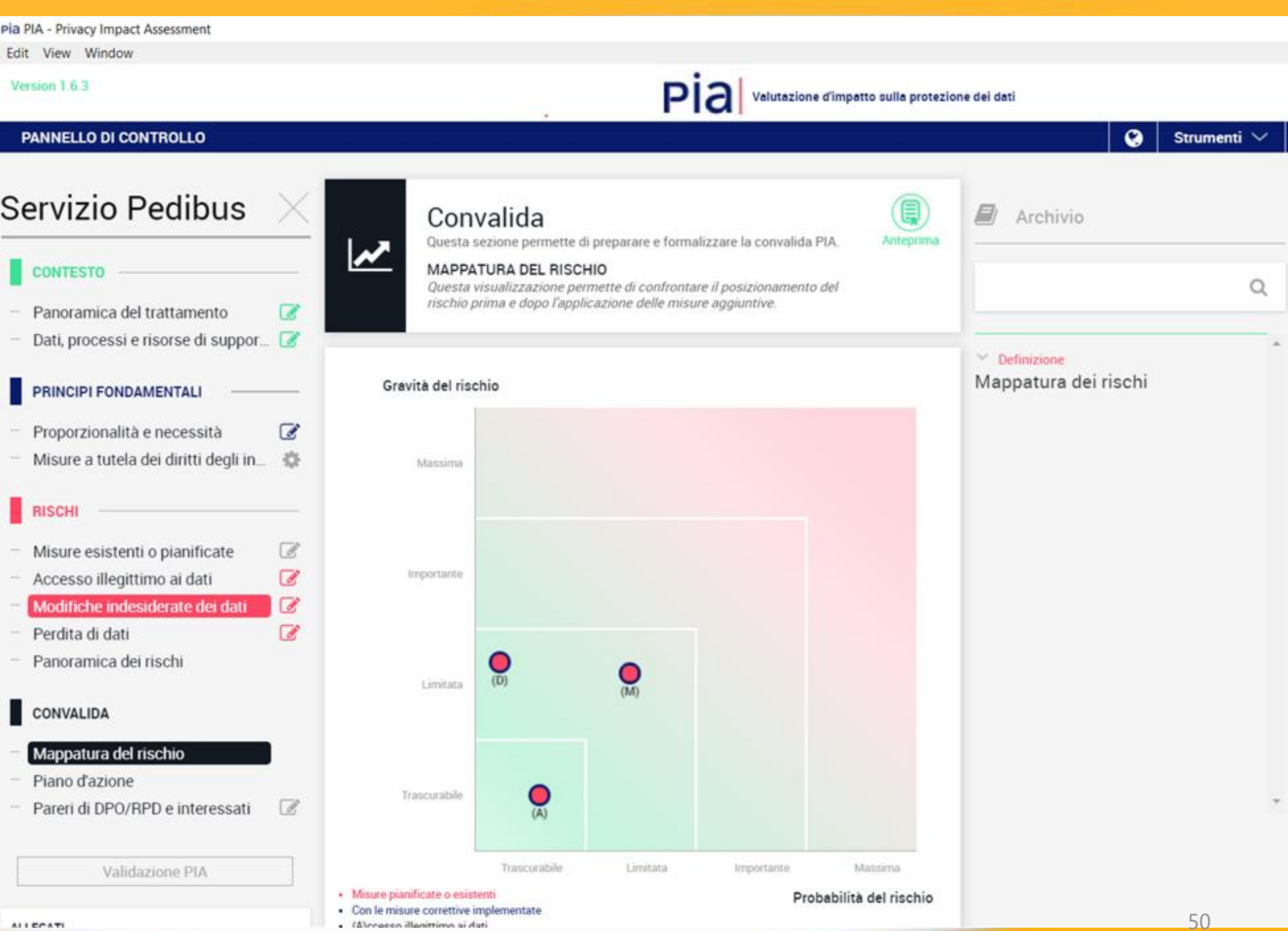
PANORAMICA DEI RISCHI

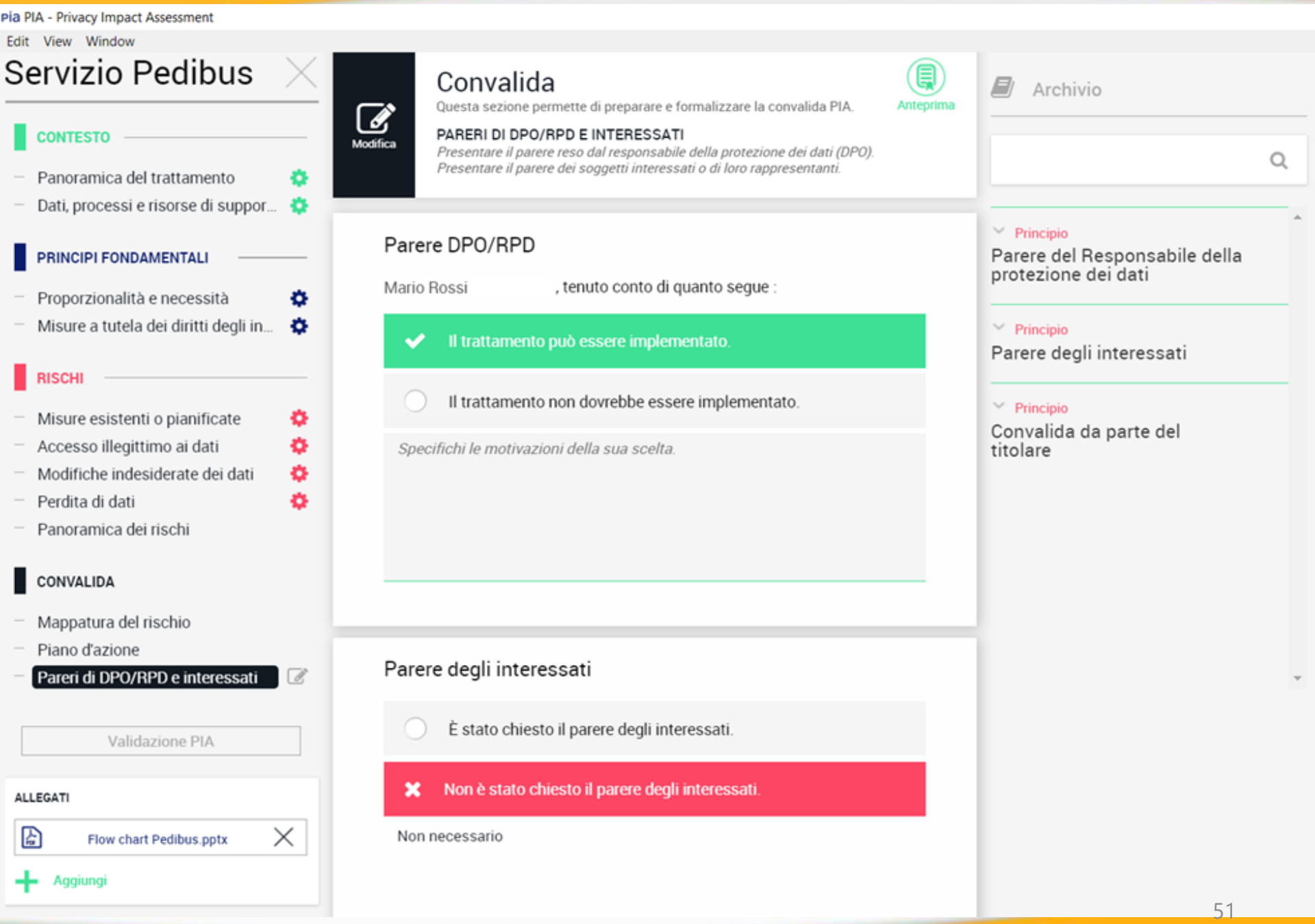
Questa visualizzazione permette una panoramica globale e sintetica degli effetti prodotti dalle misure sulle componenti di rischio che esse contribuiscono a mitigare.



Archivio

Nessun risultato trovato.


pia PIA - Privacy Impact Assessment
Edit View Window
Version 1.6.3
pia Valutazione d'impatto sulla protezione dei dati
PANNELLO DI CONTROLLO
Strumenti
Servizio Pedibus
CONTESTO
Panoramica del trattamento
Dati, processi e risorse di suppor...
PRINCIPI FONDAMENTALI
Proporzionalità e necessità
Misure a tutela dei diritti degli in...
RISCHI
Misure esistenti o pianificate
Accesso illegittimo ai dati
Modifiche indesiderate dei dati
Perdita di dati
Panoramica dei rischi
CONVALIDA
Mappatura del rischio
Piano d'azione
Pareri di DPO/RPD e interessati
Validazione PIA
Convalida
Questa sezione permette di preparare e formalizzare la convalida PIA.
MAPPATURA DEL RISCHIO
Questa visualizzazione permette di confrontare il posizionamento del rischio prima e dopo l'applicazione delle misure aggiuntive.
Anteprima
Archivio
Definizione
Mappatura dei rischi
Gravità del rischio
Massima
Importante
Limitata
Trascurabile
(D)
(M)
(A)
Trascurabile
Limitata
Importante
Massima
Probabilità del rischio
Misure pianificate o esistenti
Con le misure correttive implementate


pia PIA - Privacy Impact Assessment
Edit View Window
Servizio Pedibus
CONTESTO
Panoramica del trattamento
Dati, processi e risorse di suppor...
PRINCIPI FONDAMENTALI
Proporzionalità e necessità
Misure a tutela dei diritti degli in...
RISCHI
Misure esistenti o pianificate
Accesso illegittimo ai dati
Modifiche indesiderate dei dati
Perdita di dati
Panoramica dei rischi
CONVALIDA
Mappatura del rischio
Piano d'azione
Pareri di DPO/RPD e interessati
Validazione PIA
ALLEGATI
Flow chart Pedibus.pptx
Aggiungi
Modifica
Convalida
Questa sezione permette di preparare e formalizzare la convalida PIA.
PARERI DI DPO/RPD E INTERESSATI
Presentare il parere reso dal responsabile della protezione dei dati (DPO).
Presentare il parere dei soggetti interessati o di loro rappresentanti.
Anteprima
Parere DPO/RPD
Mario Rossi , tenuto conto di quanto segue :
Il trattamento può essere implementato.
Il trattamento non dovrebbe essere implementato.
Specifichi le motivazioni della sua scelta.
Parere degli interessati
È stato chiesto il parere degli interessati.
Non è stato chiesto il parere degli interessati.
Non necessario
Archivio
Principio
Parere del Responsabile della protezione dei dati
Principio
Parere degli interessati
Principio
Convalida da parte del titolare

Grazie per l'attenzione

rpd@sinetinformatica.it

www.sinetinformatica.it

www.sinetinformatica.it/twitter

www.sinetinformatica.it/facebook