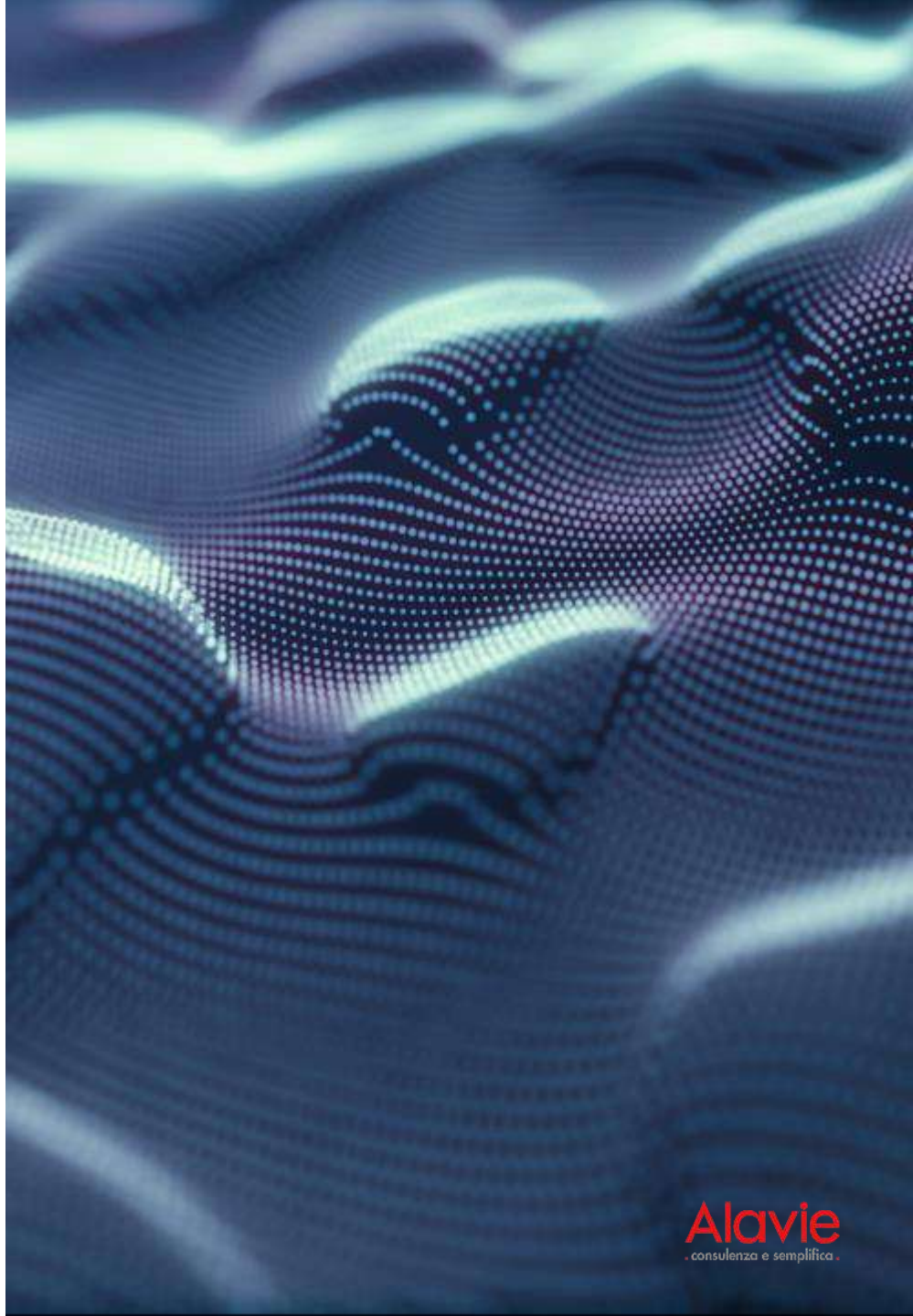
GDPR Privacy

proteggere i dati dello Studio e applicare il Dlgs 101/2018

Alavie
. consulenza e semplifica .

Contenuti del corso

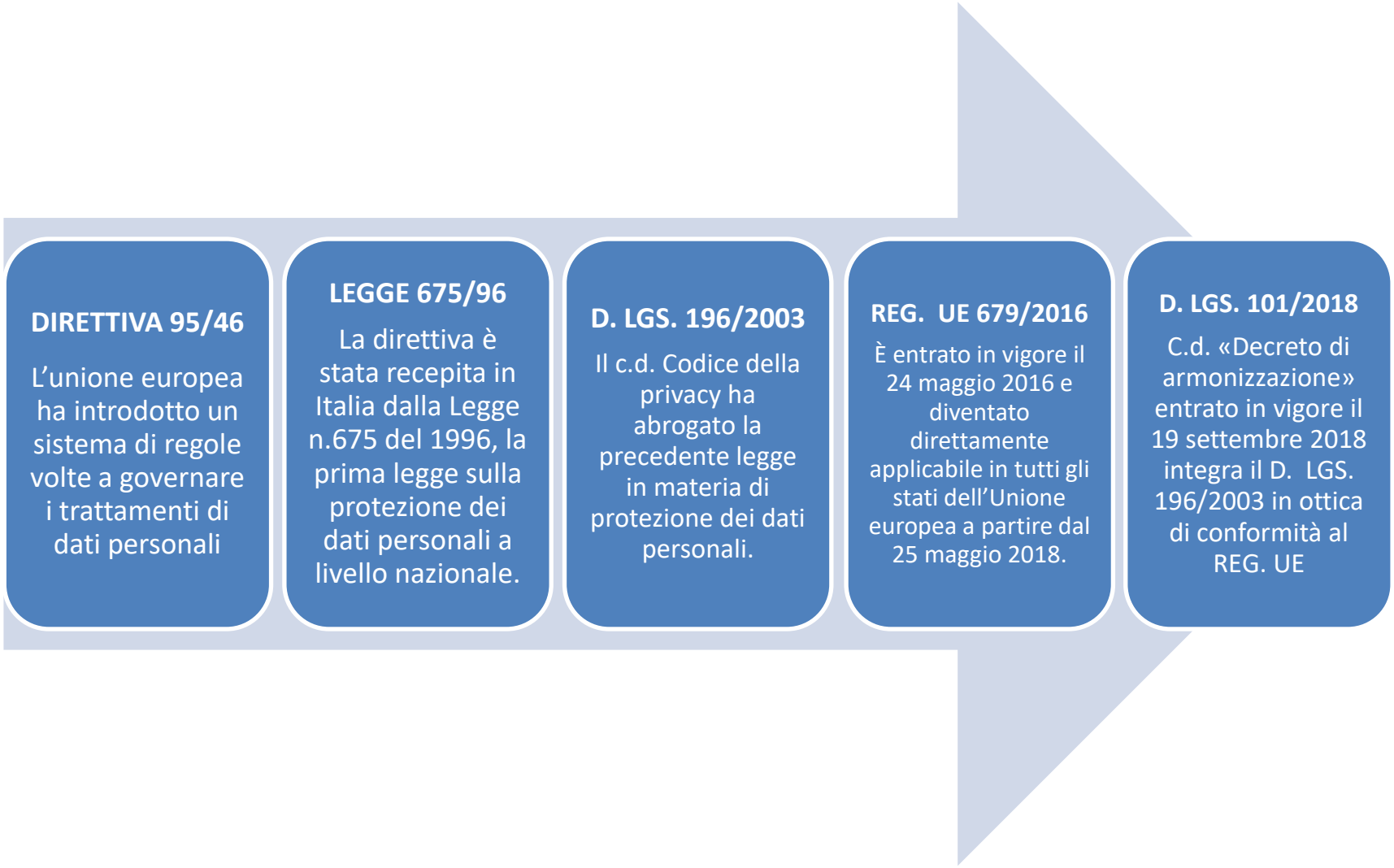
1. **Dal D.Lgs 196/2003 al Regolamento UE 2016/679**
2. Le figure del Regolamento UE 2016/679
3. Tipologie di dati ed il loro trattamento
4. Principi chiave del trattamento dei dati
5. Obblighi del titolare del trattamento
6. Vademecum e impianto sanzionatorio



Cos’è la privacy?

La protezione dei dati personali

in Italia



Alavie
consulenza e semplifica

La protezione dei dati personali

in Italia

Dal 25 maggio 2018:

Regolamento Europeo 2016/679
protezione dei dati delle persone fisiche.

D. Lgs 101/2018
In attuazione del Reg. UE 2016/679 integrando il «vecchio» D. Lgs.196/2003, in particolare:

1. Cambia **l'età minima** per prestare il consenso: 14 anni
2. Rafforza i diritti delle persone fisiche
3. Modifica l'impianto sanzionatorio

La protezione dei dati personali

in Italia

Il Legislatore non impone più il rispetto di misure minime di sicurezza

Civil Law

Ma richiede una partecipazione proattiva del Titolare del Trattamento che, conoscitore effettivo della propria realtà è chiamato a valutare **l'adeguatezza** e **l'efficacia** delle misure

Common Law

Regolamento 2016/679

L'obiettivo della nuova disciplina:
(Considerando 11, GDPR)

«un'efficace protezione dei dati personali in tutta l'Unione presuppone il rafforzamento e la disciplina dettagliata dei diritti degli interessati e degli obblighi di coloro che effettuano e determinano il trattamento dei dati personali, nonché poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali e sanzioni equivalenti per le violazioni degli Stati membri»

Alavie

Regolamento 2016/679

Principio dell'accountability
(Responsabilizzazione)

Le nuove norme responsabilizzano le figure di riferimento al quale si applica la normativa, cioè:

Il titolare del trattamento dovrà adottare un complesso sistema integrato di misure e processi giuridici, organizzativi (anche tecnologici e di formazione del personale) volte alla protezione dei dati personali

E dovrà essere in grado di dimostrarlo

Regolamento 2016/679

Alavie
consulenza e semplifica

Regolamento 2016/679

Accountability
=
Responsabilità verificabile

Art. 24 REG. UE 679/2016

Il titolare del trattamento deve mettere in atto **misure tecniche e organizzative** adeguate per garantire, **ed essere in grado di dimostrare**, che il trattamento è effettuato conformemente al Regolamento, con l'onere di riesaminarle e aggiornarle qualora necessario.

Aiutano a dimostrare la conformità l'adesione ai codici di condotta o ad un meccanismo di certificazione.

Alavie
consulenza e semplifica

Regolamento 2016/679

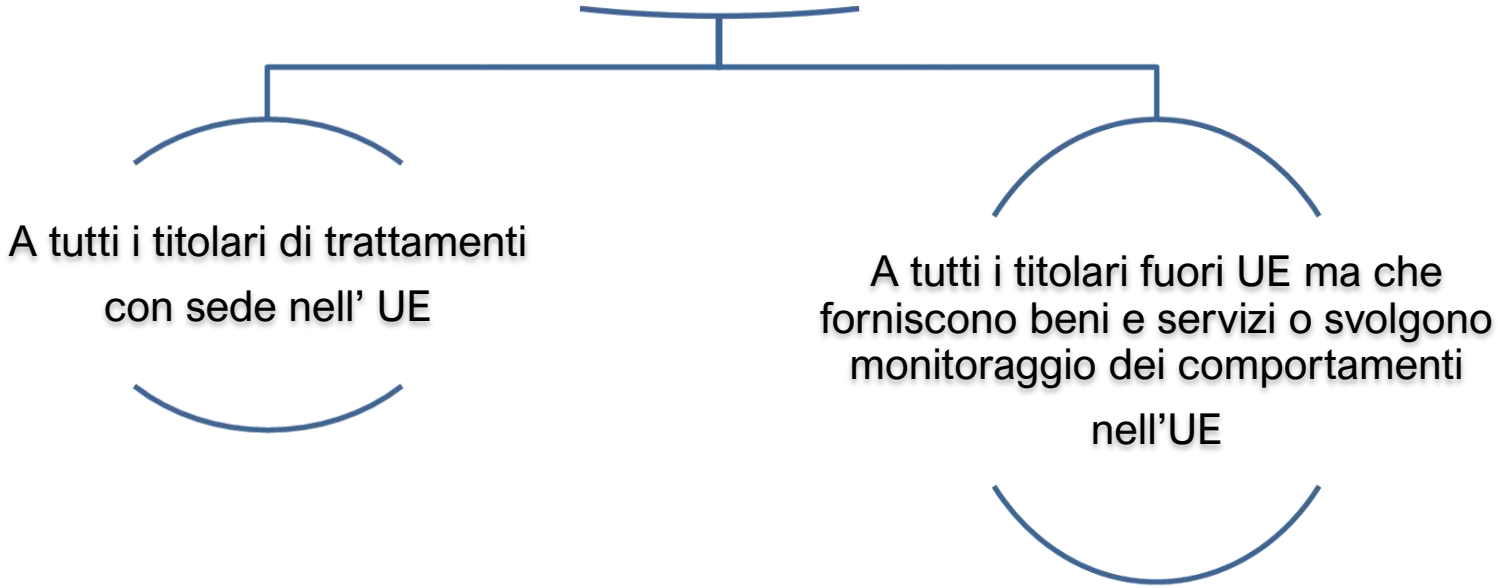
Quali persone protegge il regolamento europeo?

Solo le persone fisiche

- nel momento in cui **vengono trattati** i loro dati personali
- nel momento in cui **circolano** i loro dati personali

Regolamento 2016/679

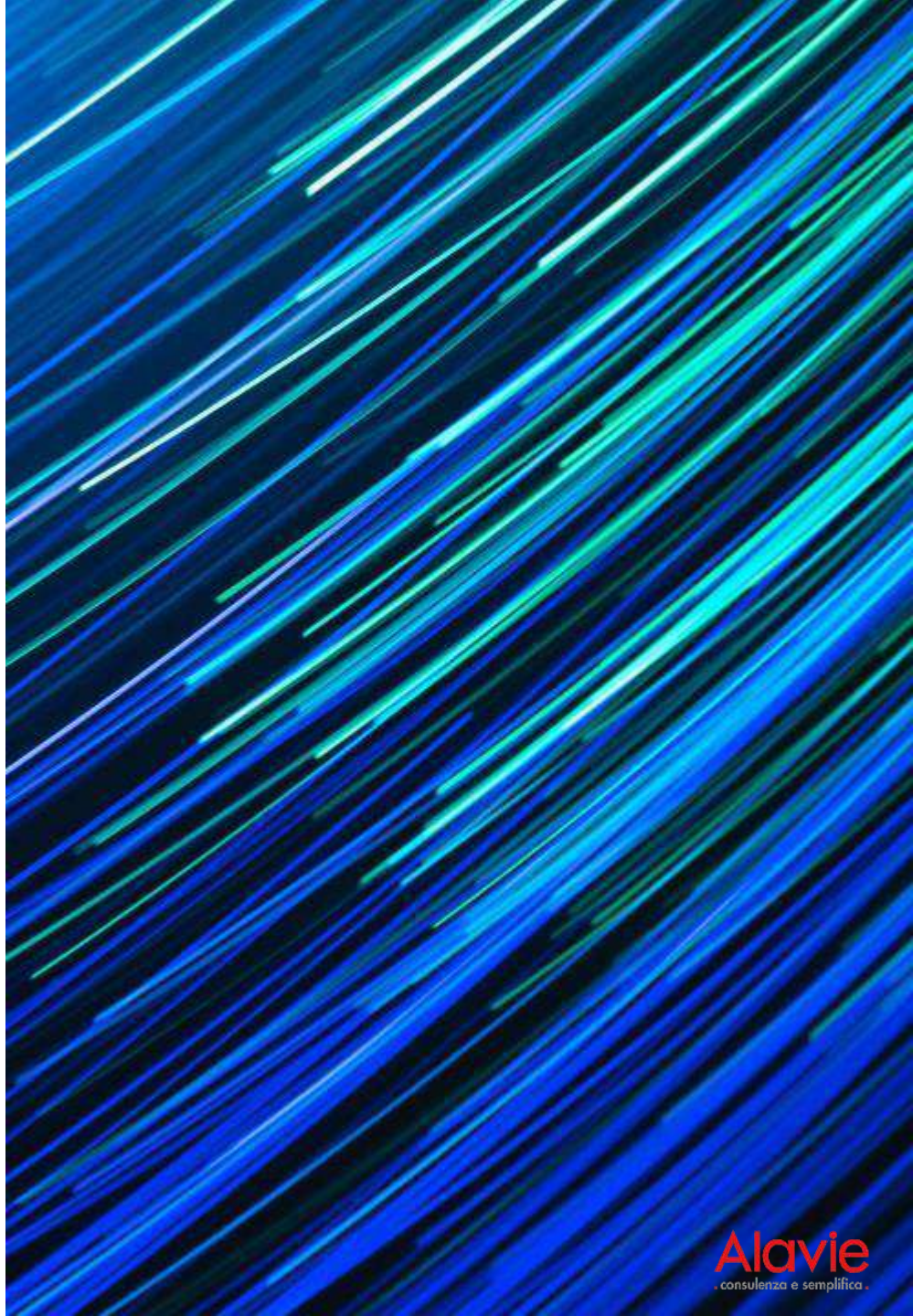
A chi si applica il nuovo regolamento europeo ?



Regolamento 2016/679

Quando non si applica il nuovo regolamento europeo?

- attività a carattere esclusivamente personale o domestico
- trattamento di dati interamente manuale in un contesto non strutturato
- Il trattamento riguarda informazioni che non sono, o non sono più, dati personali: persone decedute o dati anonimi o anonimizzati.



Regolamento 2016/679

Cosa cambia

- Ruolo del responsabile del trattamento
- Privacy by design e by default
- Valutazione dei rischi
- Adozione misure tecniche ed organizzative adeguate
- Data Breach
- Valutazione di impatto (DPIA)
- Data Protection Officer (DPO)
- Risposta all’esercizio dei diritti degli interessati
- Entità delle sanzioni

Art. 25 GDPR

Nuovo concetto «PRIVACY BY DESIGN E PRIVACY BY DEFAULT»

<<Responsabilizzazione>> delle figure principali del trattamento

adottare e rendere evidenza di comportamenti proattivi

Tali da dimostrare la concreta adozione di misure adeguate finalizzate ad assicurare l'applicazione del regolamento.

Implementare procedure ufficiali che prevedano anche:

- L'attuazione di **VALUTAZIONE D'IMPATTO** (se ed in che termini si rendano necessarie) ;
- Elaborazione di **POLICY DI STUDIO**, piani di formazione delle risorse
- interne che trattano dati, piani di audit;
- Redazione di **STANDARD DI RISPOSTA** ad eventuali richieste degli interessati;
- Previsione di un **PIANO DI COMUNICAZIONE** di violazioni dei dati personali;
- Definizione delle **MISURE DI SICUREZZA(ADEGUATE).**

Regolamento Europeo 2016/679

I principi più importanti

1. Approccio alla protezione dei dati personali basato sulla valutazione del rischio e dell'impatto
2. Maggiore responsabilizzazione di tutte le figure coinvolte
3. Obbligo di comunicare i casi di violazione dei dati personali
4. Limiti al trattamento automatizzato dei dati personali
5. Diritto di revocare Il consenso e di richiedere la cancellazione dei propri dati personali anche online
6. Diritto alla «portabilità» dei propri dati personali per trasferirli da un titolare del trattamento ad un altro

Regolamento 2016/679

Principio della «Privacy by design»

La ‘privacy’ ora incide anche sull’organizzazione della gerarchia aziendale e sulle modalità di lavoro.

Ad esempio: dovranno essere nominate figure di riferimento, designate per contratto, anche esternamente all’organizzazione.

L’ottemperanza alle norme dovrà essere costruita in MANIERA SARTORIALE.

(NO, non basta acquistare un software)

Non esistono più schemi prestabiliti.

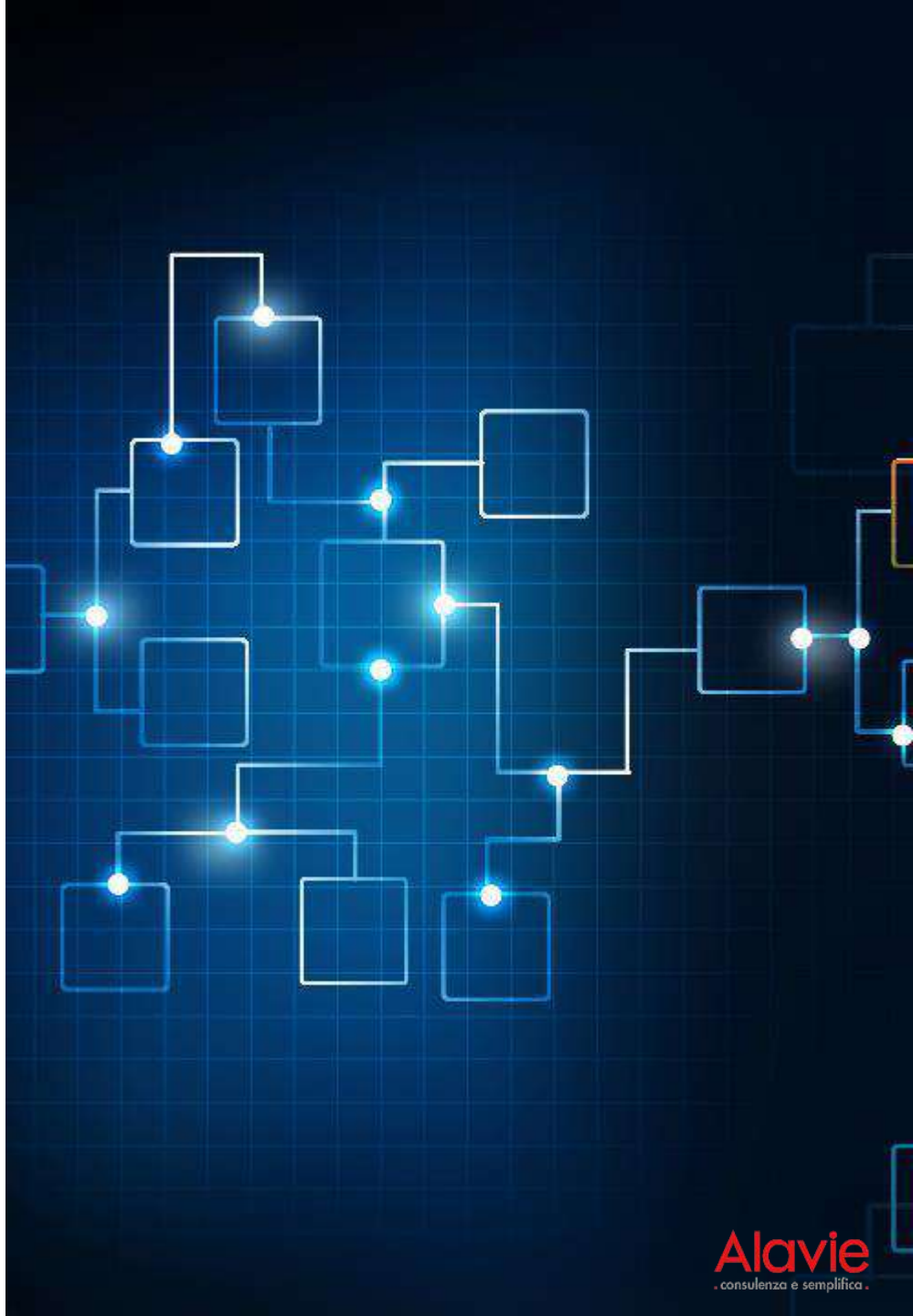
Regolamento 2016/679

Principio della «Privacy by default»

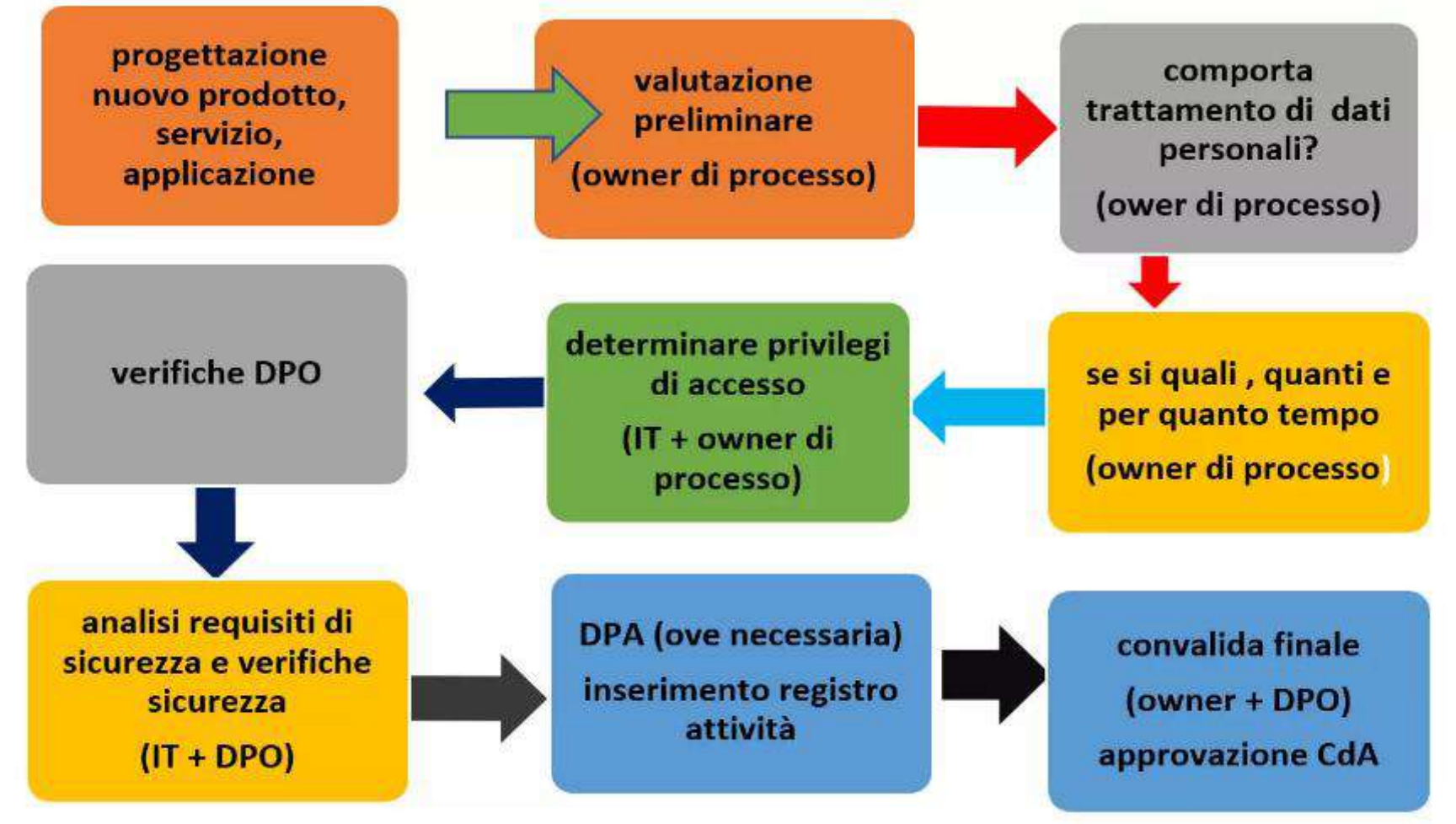
l'adeguamento alla normativa dovrà essere un'impostazione predefinita dell'organizzazione aziendale.

Ogni nuovo processo adottato, adempimento, attività svolta ecc. dovrà prevedere la protezione dei dati trattati e l'adeguamento alla normativa vigente di 'default': si tratteranno solo i dati personali strettamente necessari per le finalità che si intendono perseguire, per il tempo minimo necessario.

Alcuni casi molto banali, per capire: cambio di ufficio o di arredamento, nuove assunzioni, imprese di pulizie, cambio di server, telefoni aziendali ecc.



Regolamento 2016/679



Alavie
consulenza e semplifica

Regolamento 2016/679

Principio della «Privacy by default»

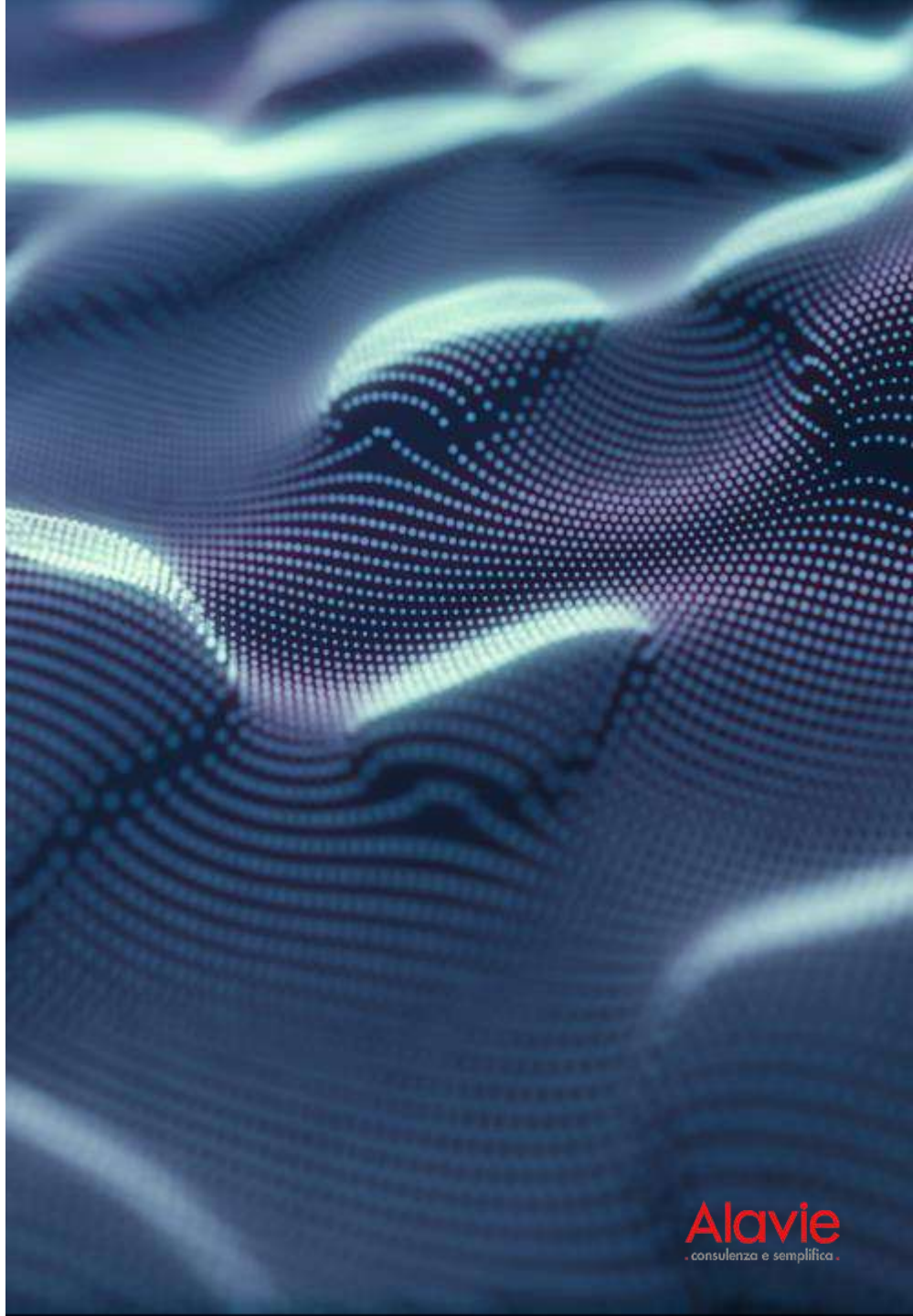
Al centro della normativa vi sono i diritti dell’interessato,
in sintonia con:

Costituzione italiana art. 2

La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale

Contenuti del corso

1. Dal D.Lgs 196/2003 al Regolamento UE 2016/679
2. **Le figure del Regolamento UE 2016/679**
3. Tipologie di dati ed il loro trattamento
4. Principi chiave del trattamento dei dati
5. Obblighi del titolare del trattamento
6. Vademecum e impianto sanzionatorio



Esame dei soggetti interessati

Esame dei soggetti interessati

TITOLARE DEL TRATTAMENTO

Persona fisica o giuridica, pubblica o privata che determina le finalità e i mezzi del trattamento dei dati personali

INTERESSATO

Persona fisica a cui si riferiscono i dati personali trattati

RESPONSABILE DEL TRATTAMENTO

Persona fisica/giuridica che può essere interno od esterno, designato tramite atto formale dal Titolare del trattamento che tratta dati personali per conto del Titolare

RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI:

È la nuova figura di garanzia per l'Autorità Garante e per il Titolare del Trattamento.
Conoscenza specialistica in materia di protezione dei dati personali e capacità di assolvere i compiti di cui all'art. 39 Reg.UE 679/2016

Alavie
consulenza e semplifica

Titolare del trattamento

Estensione dell'ambito di applicazione territoriale del GDPR:

- Titolari e responsabili stabiliti extra UE dati di interessati che si trovano in paesi UE;
- **Trasparenza**:
- Obbligo del titolare di **informare gli interessati** in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.
- In particolare nel caso di informazioni destinate ai **minori**, per consentire l'espressione di consensi validi e l'esercizio dei diritti: artt. 13 e 14.
- **Vincolo al dovere di riservatezza dei dati**, inteso come dovere di non usare, comunicare o diffondere i dati al di fuori del trattamento;
- **Documentare** le violazione dei dati personali, notificarle al Garante e **comunicarle** agli interessati nei casi previsti;
- Cooperare con l'autorità di controllo quando richiesto;

Titolare del trattamento

Responsabilizzazione del Titolare del Trattamento

(c.d. accountability):

- Obbligo di mettere in atto **misure tecniche e organizzative adeguate** che devono essere costantemente monitorate ed aggiornate;
- Per essere **in grado di dimostrare** che il trattamento è effettuato conformemente al GDPR
- Fornire le **istruzioni** al responsabile del trattamento;
- **Tenere** il registro di trattamenti;
- Fornire le istruzioni e formare **il personale (INCARICATI);**

Le figure del Reg. UE 679/2016

Definizioni art. 29 REG. UE 679/2016

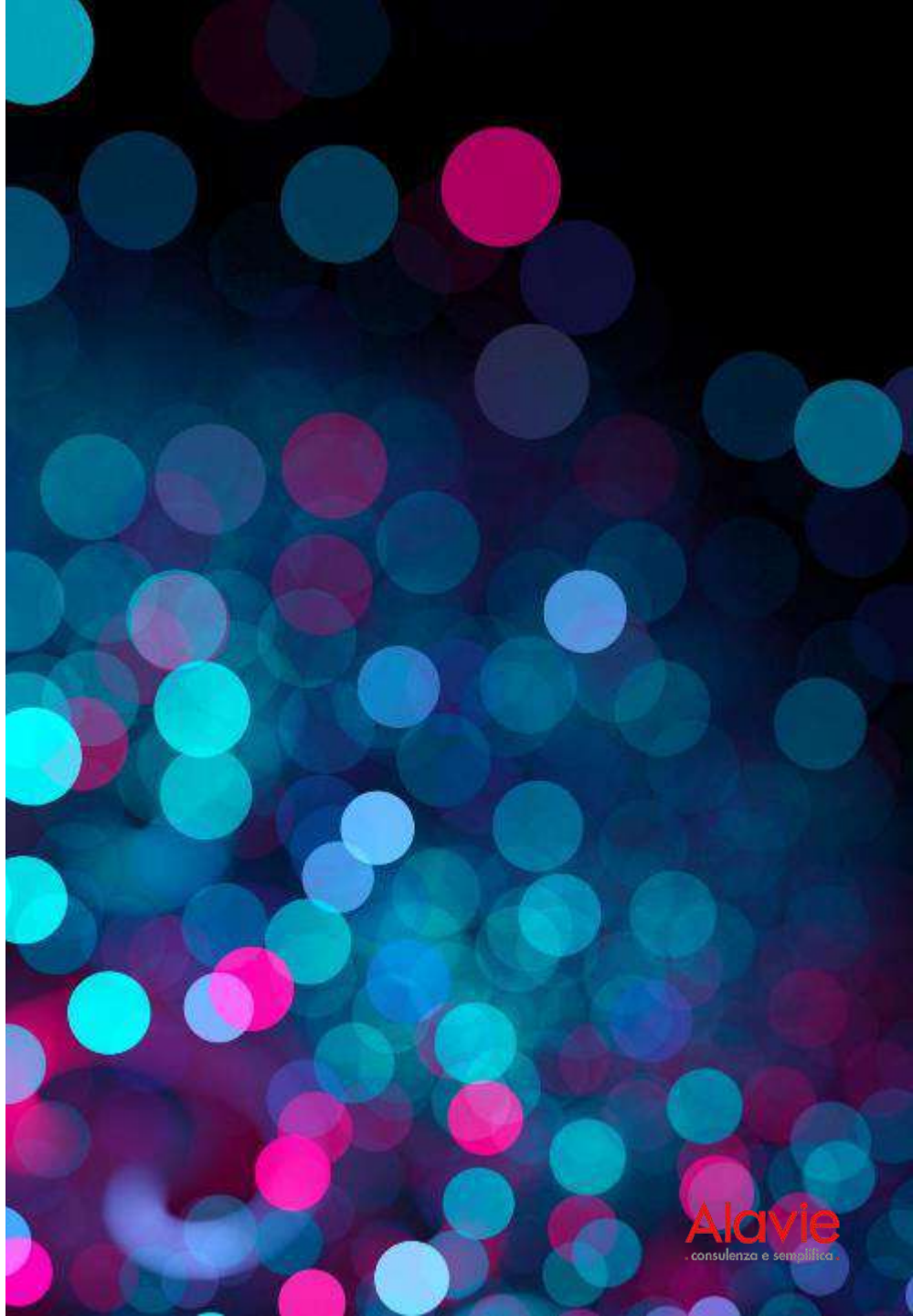
Autorizzato al trattamento

Chiunque agisca sotto l'autorità del titolare o del responsabile del trattamento non può trattare i dati se non è istruito in tal senso.

Designati *

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.

***Art. 2-quaterdecies D. Lgs. 196/2003**



Le figure del Reg. UE 679/2016

Definizioni art. 29 REG. UE 679/2016

Autorizzato

Al momento stesso dell'assunzione/inizio rapporto di lavoro, il dipendente/equipollente diventa autorizzato al trattamento dei dati personali.

Deve rispettare obblighi di riservatezza definiti dalle policy aziendali/di studio

È necessario che ne venga informato e che riceva **un'adeguata formazione.**

Le figure del Reg. UE 679/2016

Definizioni art. 29 REG. UE 679/2016

Quale ruolo svolge il consulente?

TITOLARE DEL TRATTAMENTO

- **Nel caso di cliente persona fisica** (invio telematico modello Unico PF e 730, addebito F24/F23; elaborazione ed invio telematico modello IMU; elaborazione modello ISEE; richiesta rateazione di avvisi bonari e cartelle Agenzia della Riscossione; registrazione contratti d'affitto, ecc.);
- **Per tutto quello che riguarda la gestione del proprio studio** (gestione contabile, gestione del personale, ecc.);

RESPONSABILE DEL TRATTAMENTO

- **Nel caso di cliente persona giurdica**: elaborazione dati contabili per conto dei clienti; elaborazione paghe per conto clienti.

Alavie
consulenza e semplifica

Le figure del Reg. UE 679/2016

Definizioni art. 29 REG. UE 679/2016

Responsabile esterno del trattamento

Elabora i dati personali per conto del titolare del trattamento.

È nominato tramite un atto giuridico.

Esempio: commercialista

Titolare del trattamento del Suo studio

Commercialista Dott. Bianchi

Cliente: Fioretto Srl

Responsabile del trattamento della Fioretto Srl (CONSULENZA)

I rapporti tra titolare e responsabile del trattamento

Tutti i fornitori di servizi e/o beni che sono coinvolti o che possono essere coinvolti in uno o più dei trattamenti che effettuiamo **DEVONO** essere vincolati con un **contratto** o con un altro atto giuridicamente valido.

Identificare i fornitori che dobbiamo nominare responsabili del trattamento

Alavie
consulenza e semplifica

Nomina del responsabile del trattamento (art. 28)

PREMESSA

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

Alavie
consulenza e semplifica

Nomina del responsabile del trattamento (art. 28)

Obblighi del responsabile del trattamento (art. 28.3)

a) trattare i dati solo su istruzioni documentate del titolare;

b) assicurare che gli incaricati si siano impegnati alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adottare tutte le misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio ai sensi dell'art. 32;

d) ricorrere ad un altro responsabile (SUBRESPONSABILE) solo previa autorizzazione scritta, specifica o generale, del titolare del trattamento;

e) assistere il titolare con adeguate misure, tecniche ed organizzative, per «dar seguito alle richieste per l'esercizio dei diritti dell'interessato»;

Alavie
consulenza e semplifica

Nomina del responsabile del trattamento (art. 28)

Obblighi del responsabile del trattamento (art. 28.3)

f) assistere il titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 (misure tecniche, data breach, dpia), tenuto conto della natura del trattamento e delle informazioni a disposizione del Responsabile;

g) cancellare tutti i dati personali o restituire le copie esistenti alla cessazione delle funzioni di Responsabile;

h) mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto dei propri obblighi e collaborazione alle attività di revisione, comprese le ispezioni realizzate dal Titolare o da un altro soggetto da questi incaricato. Il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

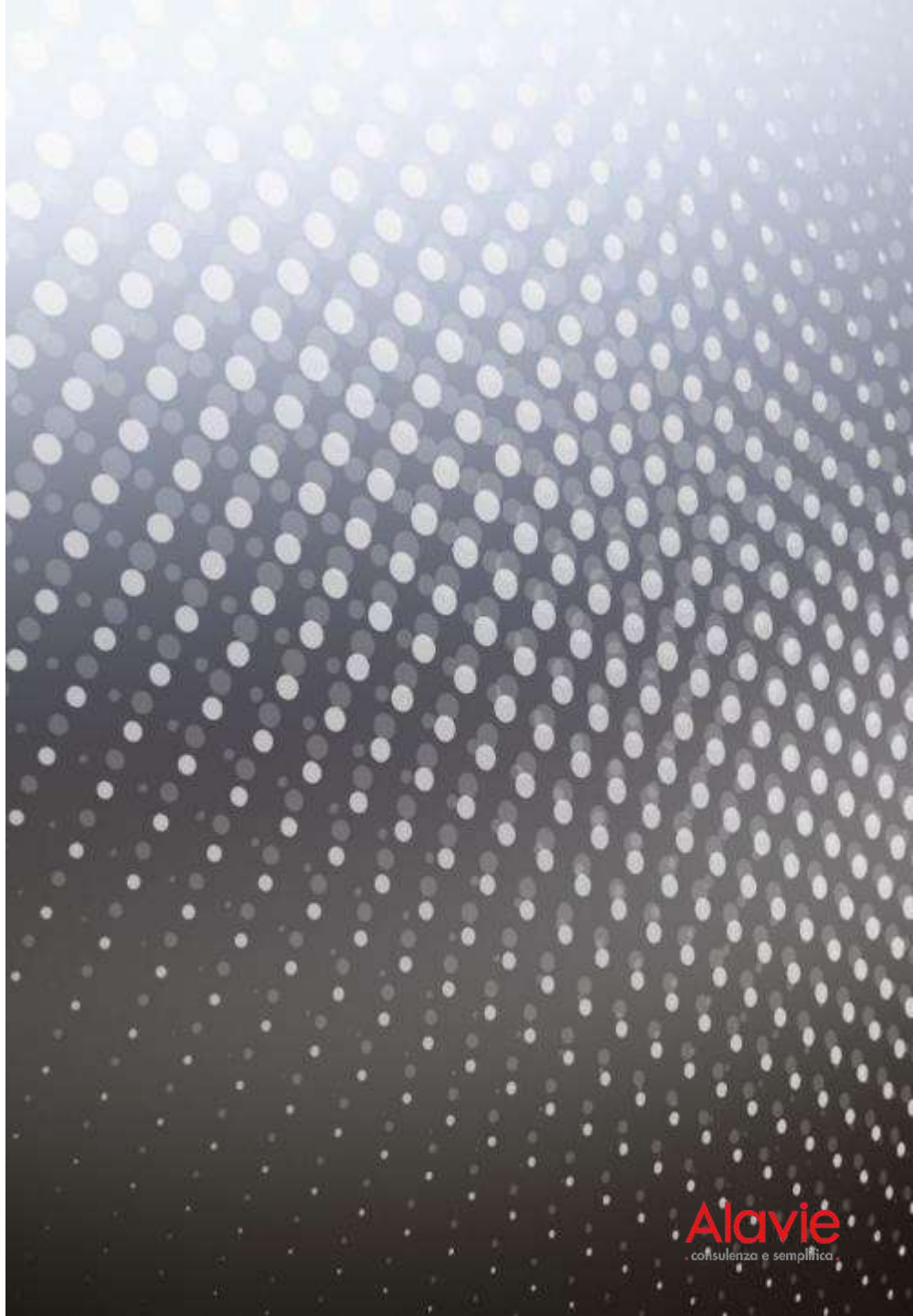
I rapporti tra titolare e responsabile del trattamento

Tutti i fornitori di servizi e/o beni che sono coinvolti o che possono essere coinvolti in uno o più dei trattamenti che effettuiamo DEVONO fornirci valide garanzie per dimostrare che il trattamento che affidiamo loro sarà sicuro e non sarà fonte di rischi inadeguati o insostenibili per noi e per gli interessati

Come?

1. Farsi dare le evidenze della conformità al GDPR e della sicurezza dei trattamenti affidati;

2. Attività di audit/assessment.



I sub-responsabili

Il responsabile può nominare sub-responsabili per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e «responsabile primario».

ATTENZIONE:

Il «responsabile primario» risponde dinanzi al titolare dell'inadempimento del sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento.

Le figure del Reg. UE 679/2016

Definizioni art. 29 REG. UE 679/2016

DPO (Data Protection Officer) Art. 37 - 38 - 39

Trattamento effettuato da autorità pubblica o da un organismo pubblico , eccetto autorità giurisdizionali

Per tutti i soggetti (enti e imprese) che trattano dati sensibili su larga scala

Obbligatorio

Per tutti i soggetti (enti e imprese) che effettuano monitoraggio regolare e sistematico su larga scala

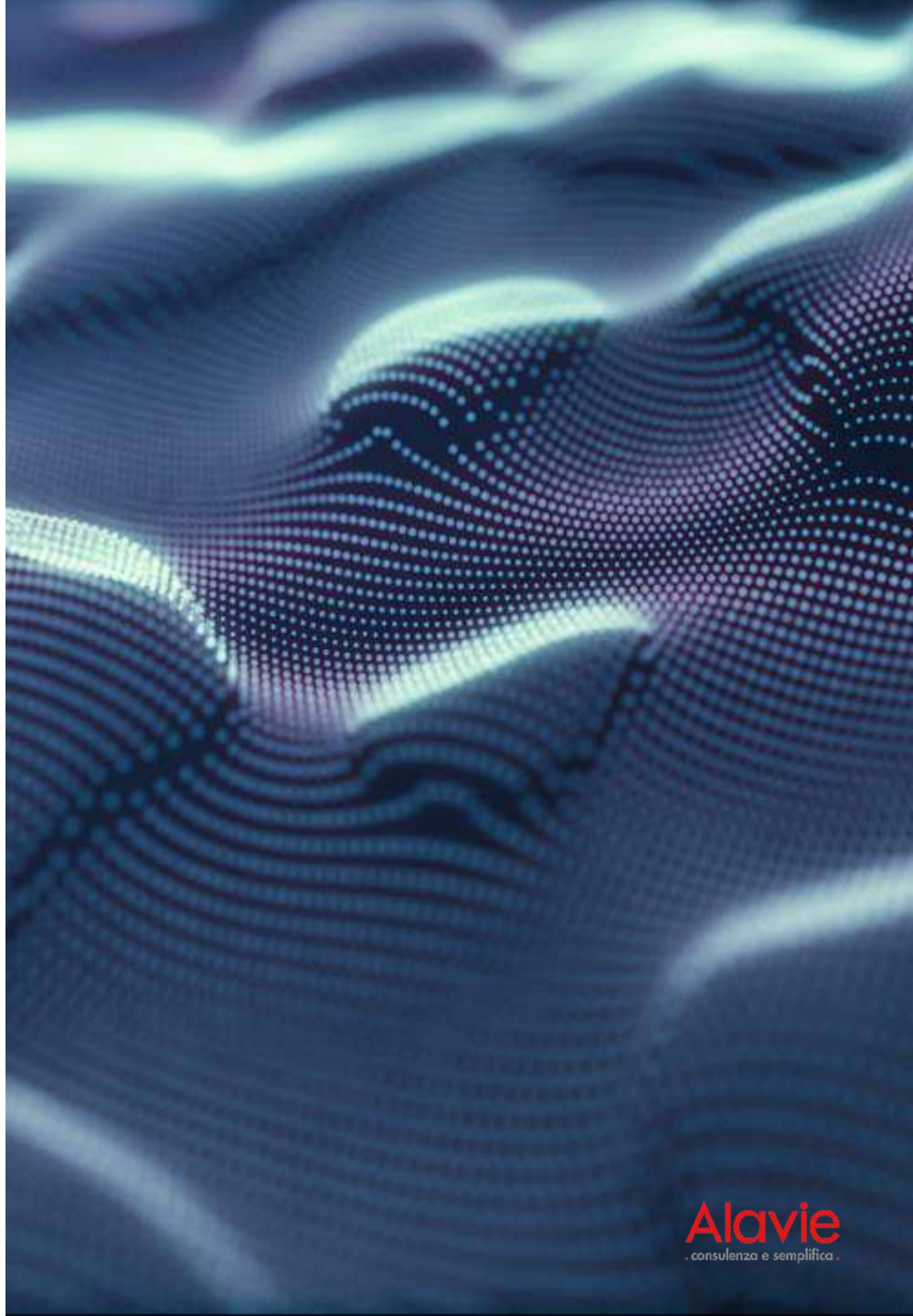
Designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati, e della capacità di adempiere ai compiti.

Le figure del Reg. UE 679/2016

Alavie
consulenza e semplifica

Contenuti del corso

1. Dal D.Lgs 196/2003 al Regolamento UE 2016/679
2. Le figure del Regolamento UE 2016/679
3. **Tipologie di dati ed il loro trattamento**
4. Principi chiave del trattamento dei dati
5. Obblighi del titolare del trattamento
6. Vademecum e impianto sanzionatorio

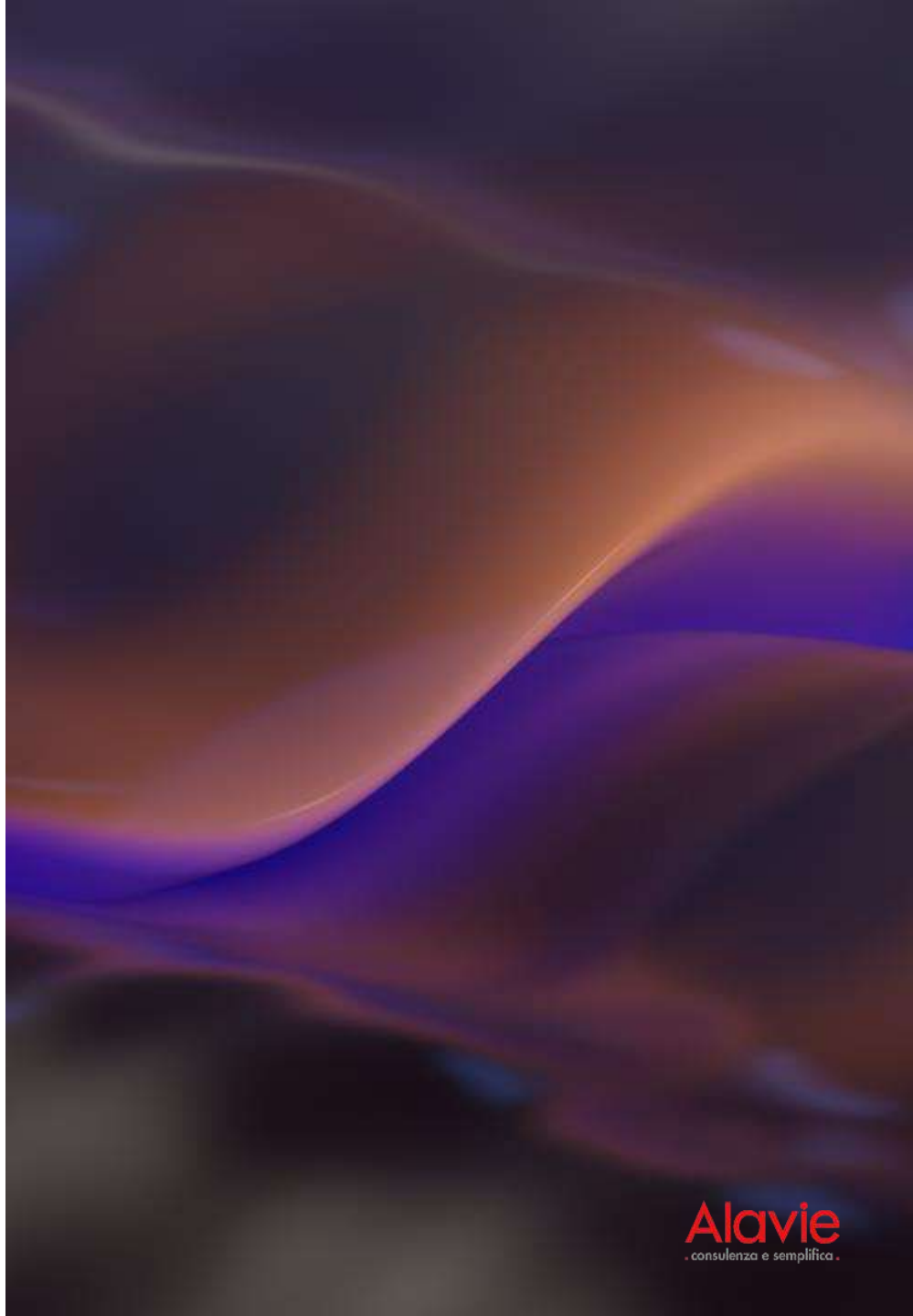


Cos’è un trattamento di dati personali?

Definizioni art. 4 REG. UE 679/2016

Qualsiasi attività svolta su dati personali, anche di tipo non trasformativo quale ad esempio un mero accesso.

Il Garante italiano ha considerato pacificamente la videosorveglianza senza registrazione come una tipologia di trattamento, prescrivendo di conseguenza modalità e attenzioni per la sua effettuazione.



Trattamento di dati – che cos’è?

Qualsiasi operazione o insieme di operazioni, compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, ad esempio:

- Raccolta
- Registrazione
- Organizzazione
- Strutturazione
- Conservazione
- Adattamento o la modifica
- Estrazione
- Consultazione
- Uso
- Comunicazione mediante trasmissione
- Diffusione o qualsiasi altra forma di messa a disposizione
- Raffronto o interconnessione
- Limitazione
- Cancellazione o distruzione

Cos’è un dato personale?

Definizioni art. 4 REG. UE 679/2016

Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»);

si considera identificabile la persona che può essere identificata, direttamente o indirettamente, con particolare riferimento ad un identificativo come il nome, un numero di identificazione, dati relativi all’ubicazione, un identificativo on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Sono dati personali

indirizzo IP

soprannome

ubicazione della persona fisica

account

comportamenti abituali

dati del conto corrente

descrizione fisica della persona

le risposte tipiche in certe situazioni

dati della carta di credito

Categorie particolari di dati

Definizioni art. 4 REG. UE 679/2016

Dati genetici

Dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona che forniscono informazioni uniche sulla fisiologia o sulla salute di detta persona, in particolare dall'analisi di un campione biologico.

Dati biometrici:

i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dati relativi alla salute:

i dati personali attinenti alla salute fisica o mentale di una persona, compresa la prestazione di servizi di assistenza sanitaria, che rivelino informazioni relative al suo stato di salute.

Dati sensibili:

origine etnica e razziale, opinioni politiche, convinzioni filosofiche e religiose, l'appartenenza sindacale, dati relativi alla vita sessuale o orientamento sessuale.

Foto/selfie sul lavoro innocui ?

Foto di un arresto o di un fermo da parte della polizia ….

Trattamento di dati giudiziari

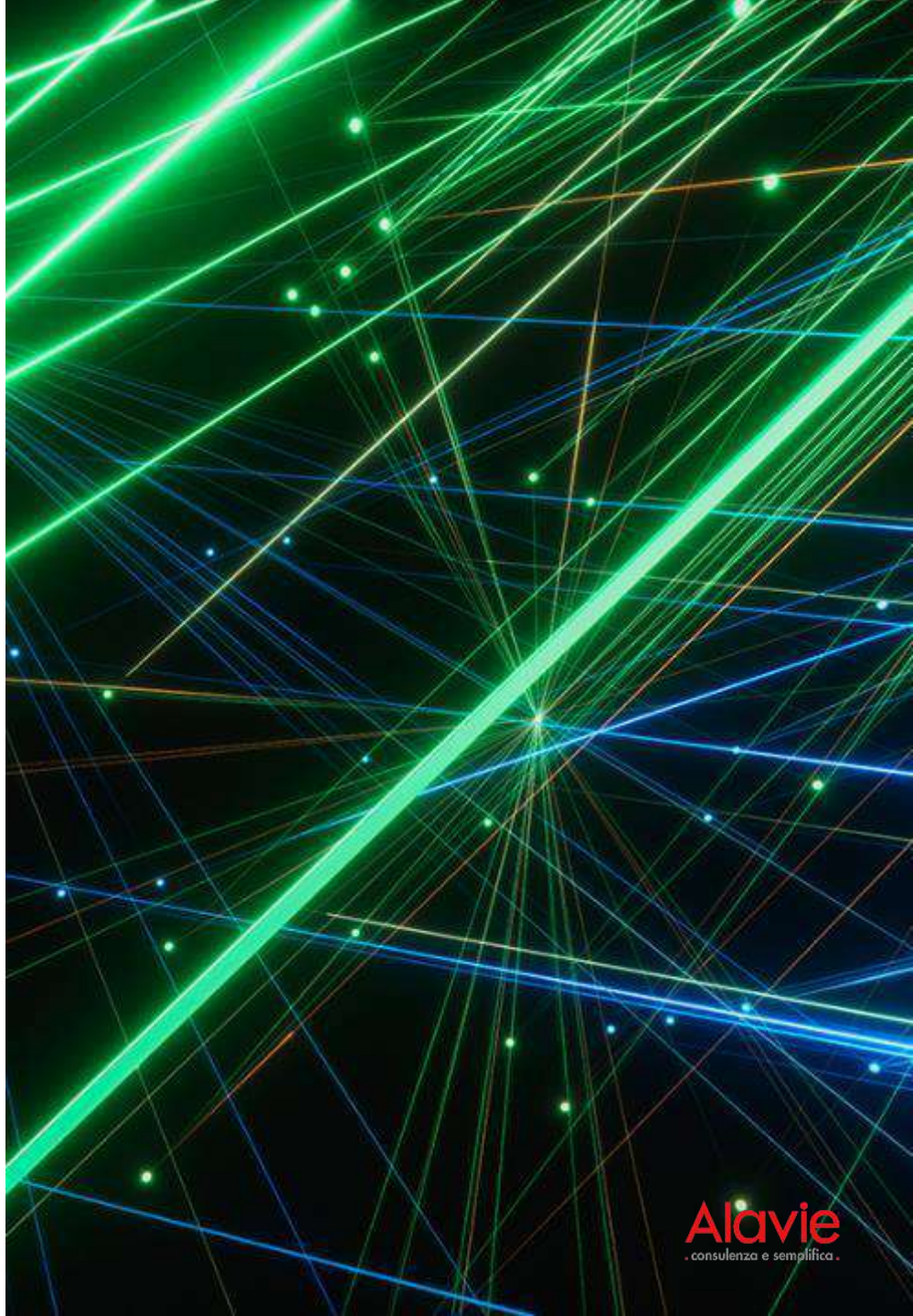
Foto con dei figli minorenni di colleghi o clienti …

Trattamento di dati personali di minori

Un bel selfie durante una visita in ospedale …

Trattamento di dati particolari relativi alla salute

Anche dati personali ordinari, qualora associati ad altre informazioni, potrebbero essere idonei a rivelare una delle condizioni inerenti ai dati particolari e assumere dunque la qualifica di dato particolare.



Il consenso

Per attività extra contrattuali

Caratteristiche:

Libero/

Non condizionato

Esplicito

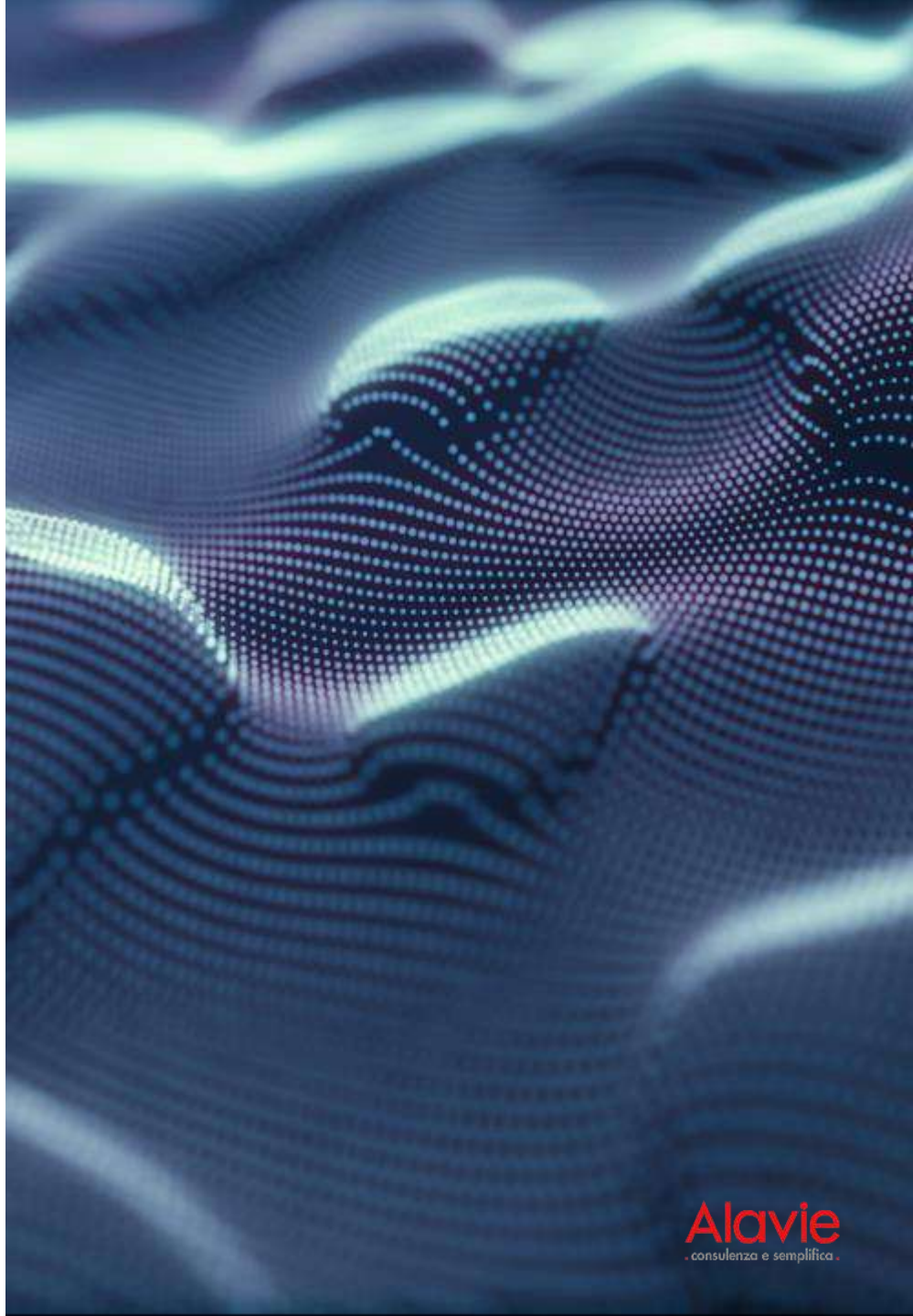
Dimostrabile

Principio di accountability

Alavie
consulenza e semplifica

Contenuti del corso

1. Dal D.Lgs 196/2003 al Regolamento UE 2016/679
2. Le figure del Regolamento UE 2016/679
3. Tipologie di dati ed il loro trattamento
4. **Principi chiave del trattamento dei dati**
5. Obblighi del titolare del trattamento
6. Vademecum e impianto sanzionatorio



Come devono essere trattati i dati personali?

- In modo **lecito, corretto e trasparente** nei confronti dell'interessato;
- Raccolti per **finalità determinate, esplicite e legittime**;
- **Adeguati, pertinenti e limitati** a quanto necessario;
- **Esatti** e, se necessario, **aggiornati**;
- **Conservati** in una forma che consenta l'identificazione degli interessati **per un arco di tempo non superiore** al conseguimento delle finalità per le quali sono trattati;
- **Trattati in maniera da garantire un'adeguata sicurezza** dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Finalità determinate, esplicite e legittime

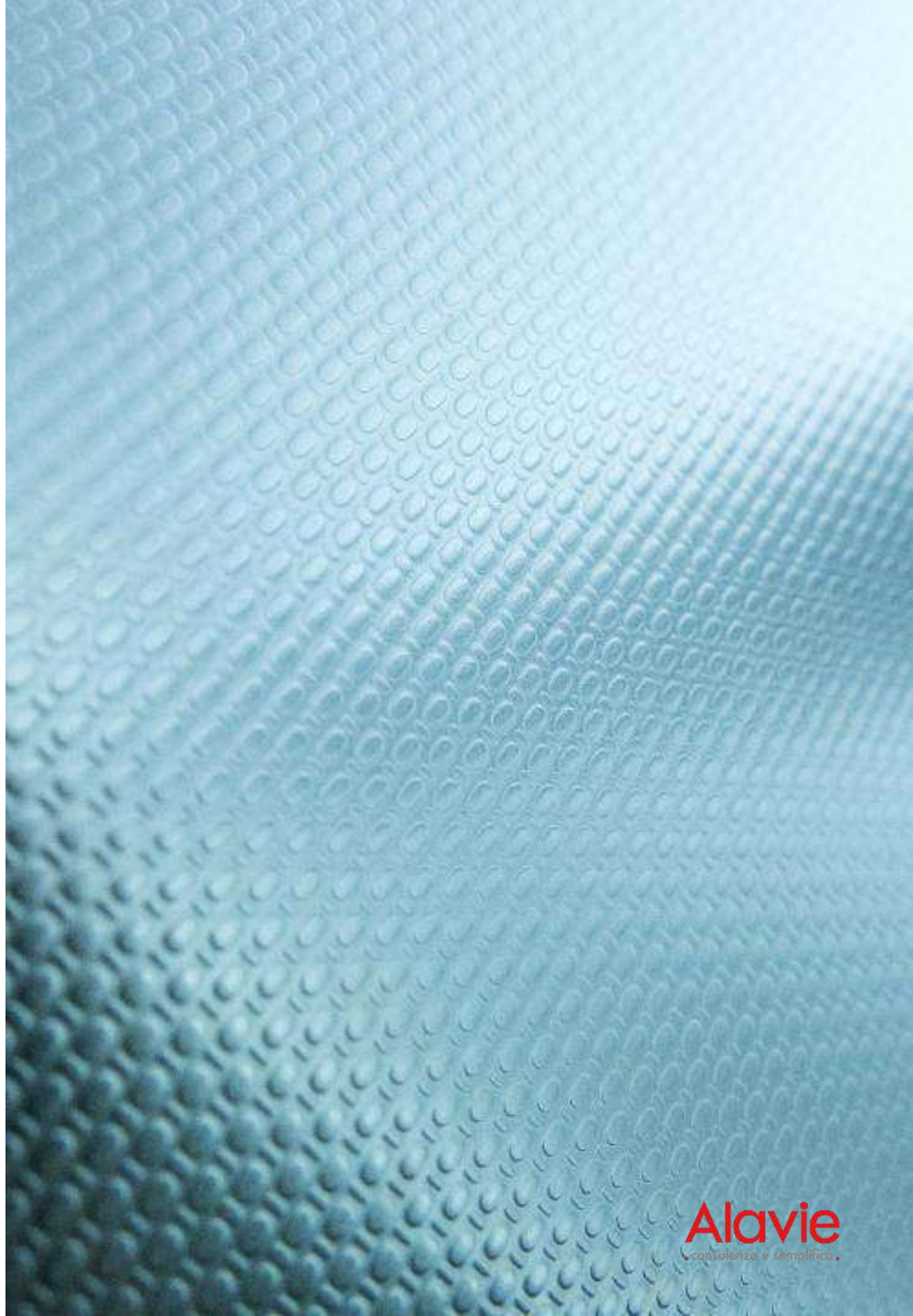
I dati personali devono essere raccolti per finalità:

- Determinate (cioè chiare ed esaustive)
- Esplicite (cioè espressamente manifeste)
- Legittime (non in contrasto con la legge).

Un ulteriore trattamento dei dati personali ai fini diversi da quelli stabiliti inizialmente è considerato incompatibile

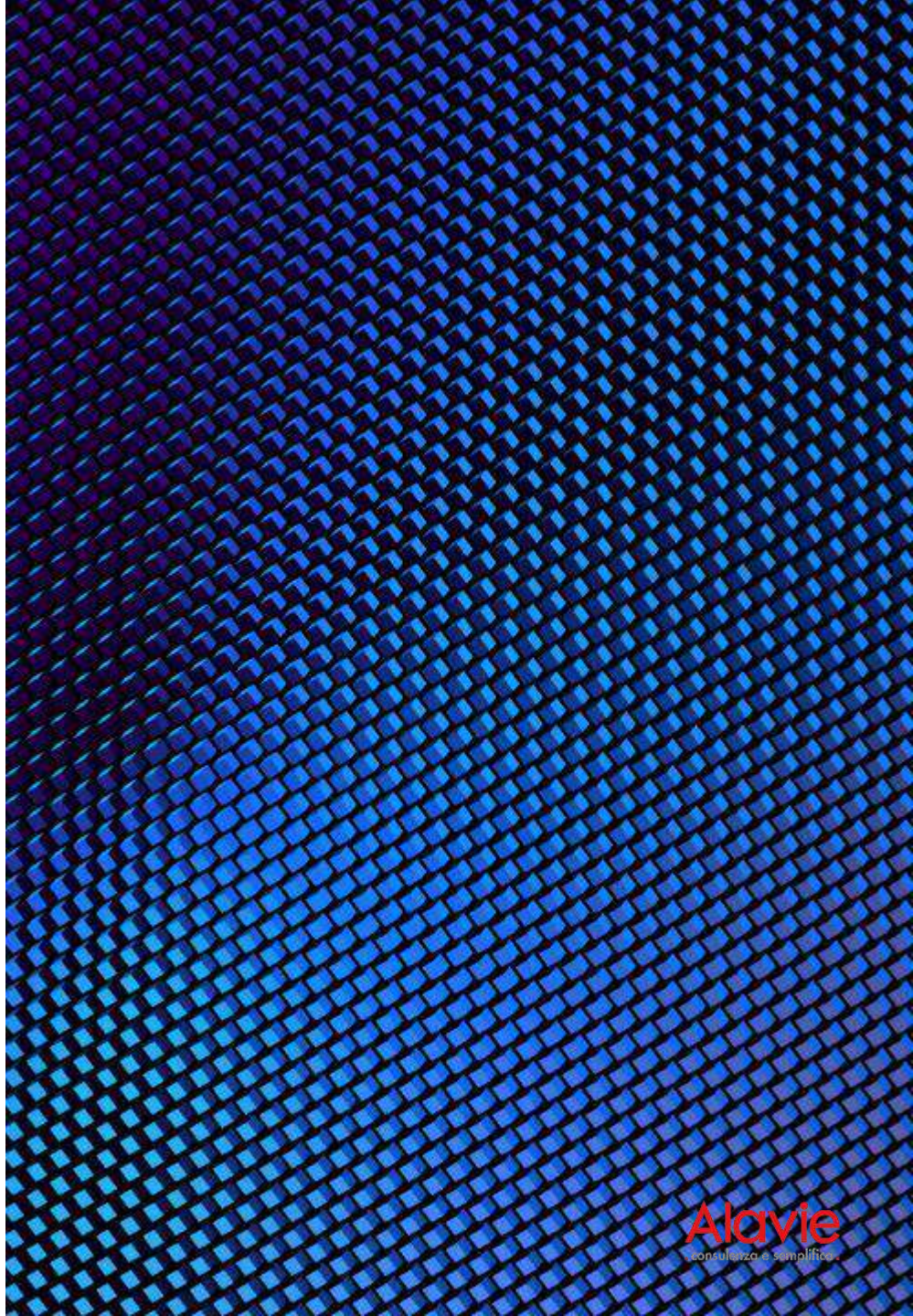
Quando è lecito un trattamento?

- **L'interessato ha espresso il consenso al trattamento** dei propri dati personali per una o più finalità.
- Il trattamento è **necessario all'esecuzione di un contratto** di cui l'interessato è parte […];
- è necessario per **adempiere un obbligo legale del titolare**;
- è necessario per la **salvaguardia di interessi vitali di una persona fisica**;
- è necessario per **l'esecuzione di un compito di interesse pubblico** o connesso con l'esercizio di pubblici poteri;
- è necessario per il **perseguimento di un legittimo interesse del titolare** o di terzi, a condizione che non prevalgano sui diritti/libertà dell'interessato.



Quando è lecito un trattamento di dati particolari?

- Consenso esplicito per finalità specifiche;
- necessità di osservare obblighi in materia di diritto del lavoro, sicurezza e protezione sociale;
- trattamento di interesse vitale dell'interessato o di altra persona;
- trattamento effettuato da organismo non lucrativo con finalità politiche, filosofiche , religiose, sindacali;
- Dati resi manifestamente pubblici dall'interessato;
- Necessità di accertare, esercitare, difendere un diritto in sede giudiziaria;
- Interesse pubblico sulla base dell'ordinamento europeo o interno; trattamenti sanitari, ricerca scientifica e storica, statistica.



Condizioni per il consenso

Definizioni art. 29 REG. UE 679/2016

INEQUIVOCABILE

Qualsiasi manifestazione di volontà libera, specifica, informata con il quale l'interessato manifesta il proprio assenso

GRANULARE

Quando Il consenso sia fornito in una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre tematiche trattate

REVOCABILE

Il diritto di revoca è
Previsto in ogni momento.
La revoca del consenso non pregiudica la liceità del trattamento basato sul consenso fornito prima della revoca

Alavie
consulenza e semplifica

Contratto e consenso

L’adesione ad un servizio di posta elettronica non prevede per l’interessato che ne faccia richiesta l’espressione di un consenso al trattamento dei dati personali necessari per il funzionamento del servizio stesso.

Per esempio, nome, cognome, codice fiscale, indirizzo di fatturazione, ecc.

Tuttavia, se il fornitore del servizio, intenda usare le coordinate di posta elettronica per l’invio di una newsletter informativa periodica all’interessato, avrà bisogno di acquisire preventivo consenso al trattamento.

Principi chiave

NON ECCEDENZA, ADEGUATEZZA, PERTINENZA, MINIMIZZAZIONE, DATA RETENTION: bisogna ridurre al minimo l'uso di dati personali; devono essere pertinenti ed adeguati rispetto alle finalità perseguite; conservati per il tempo minimo necessario;

LICEITÀ E CORRETTEZZA: il trattamento deve avvenire in maniera lecita e corretta informando i soggetti interessati circa la raccolta, l'utilizzo e la consultazione dei loro dati o ulteriori tipologie di trattamenti, ecc.

TRASPARENZA: le informazioni e le comunicazioni devono essere facilmente accessibili e comprensibili, utilizzando un linguaggio semplice e chiaro;

Minimizzazione

È vietato l’uso dei dati personali quando non sono assolutamente necessari o quando è possibile ottenere lo stesso risultato tramite l’uso di dati anonimi.

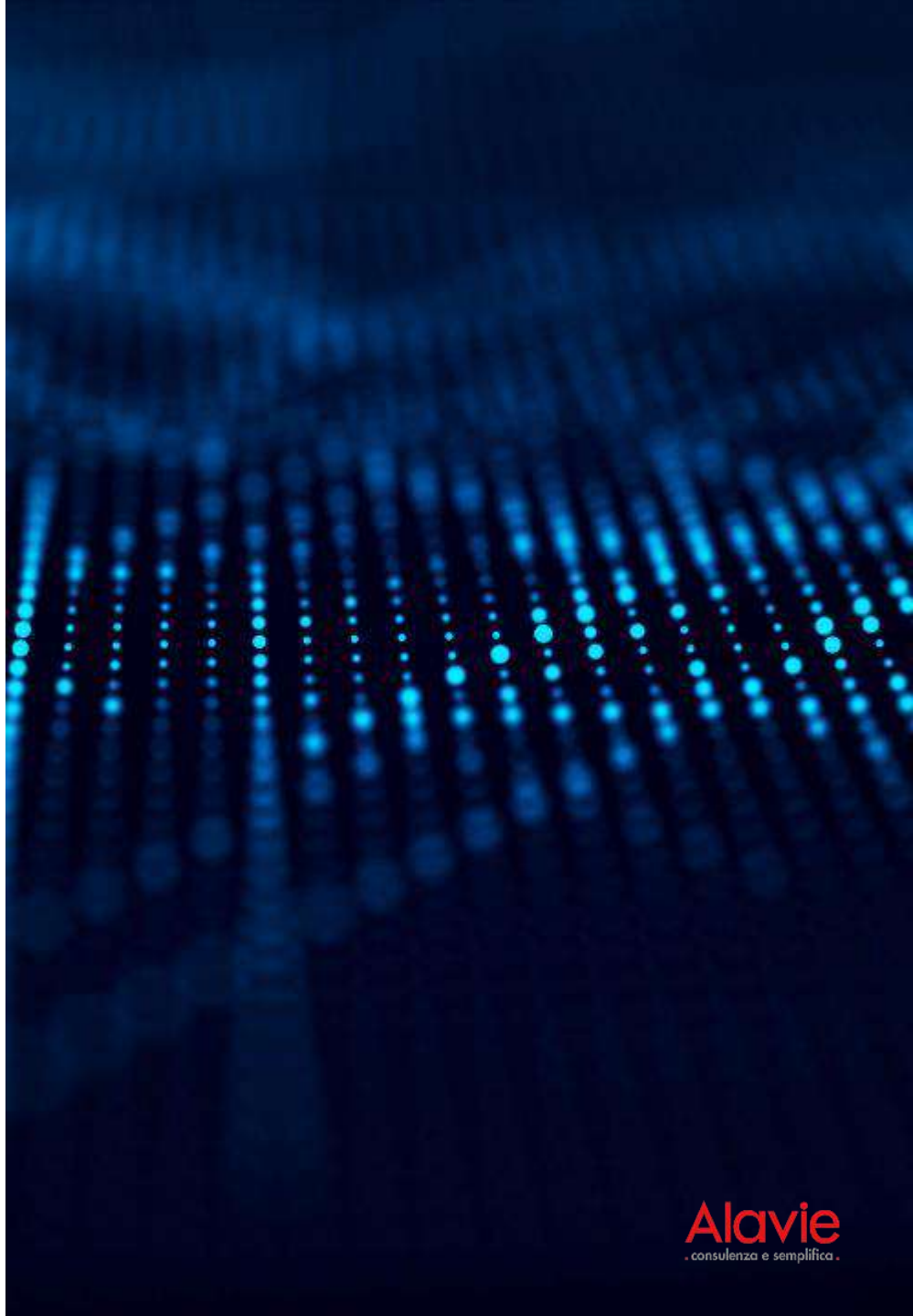
Minimizzazione

Caso pratico

Provvedimento del Garante Privacy

Sito di commercio elettronico:
la visualizzazione di proposte commerciali era subordinata al completamento di una **procedura di registrazione** nella quale l'utente era tenuto a fornire il proprio indirizzo di posta elettronica e ad accettare i termini e condizioni e la privacy policy.

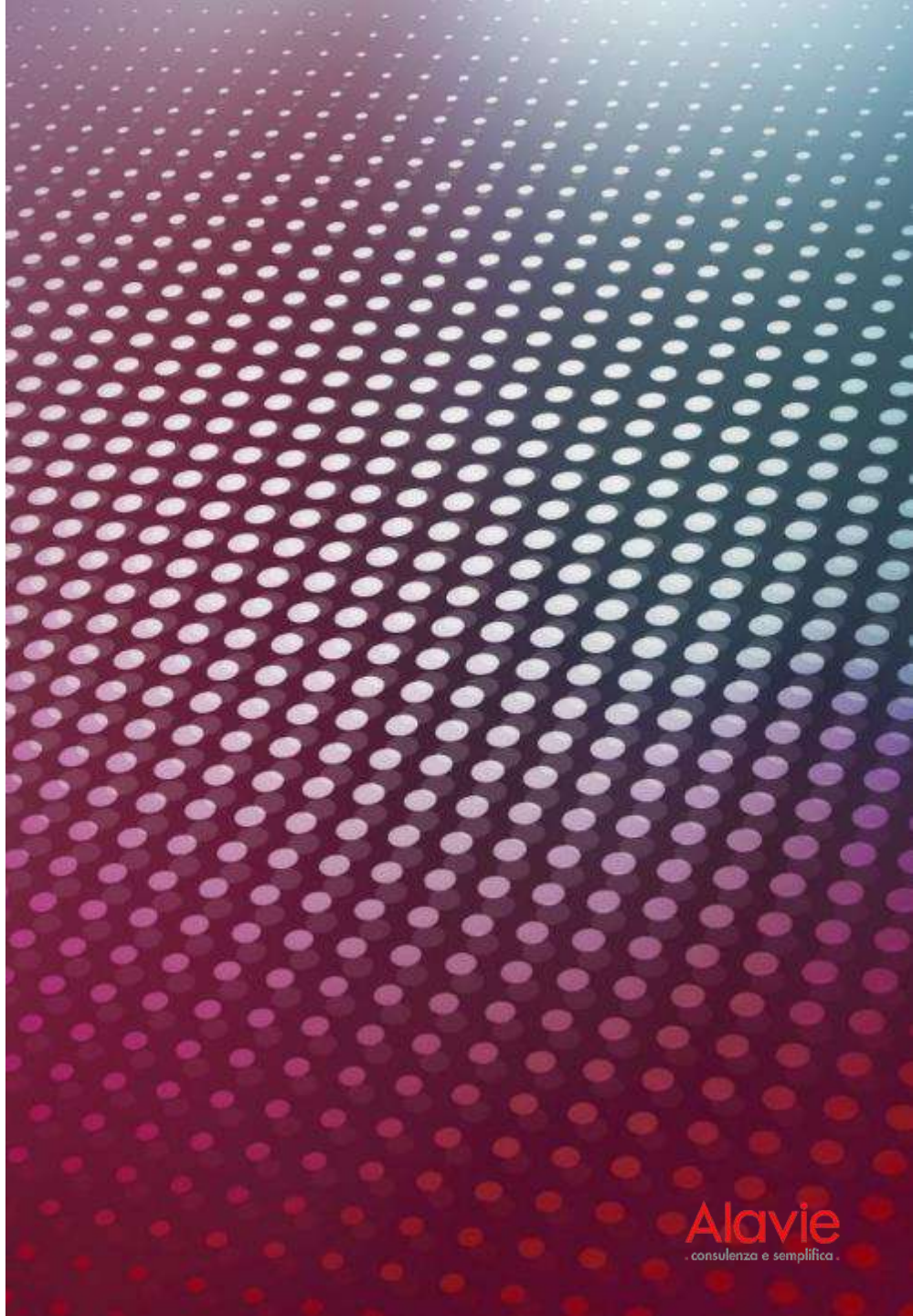
Il Garante così si esprime:
"il trattamento dell'informazione relativa all'indirizzo di posta elettronica non può ritenersi necessario per consentire la "navigazione" nel sito web e la conseguente visualizzazione delle proposte commerciali ivi contenute"



Conservazione e durata

La conservazione dei dati personali è consentita per un arco di tempo definito, non superiore al conseguimento delle finalità del trattamento

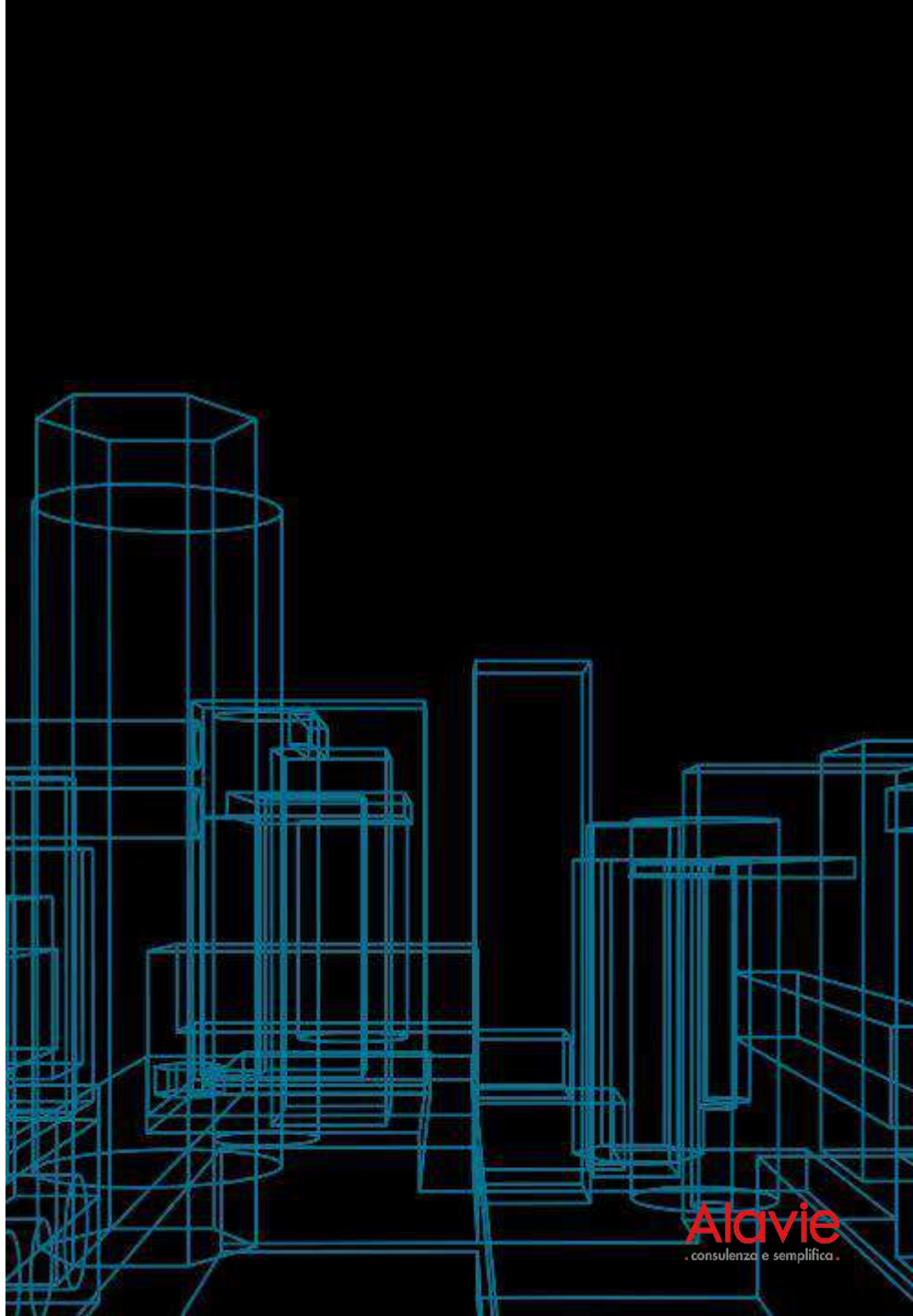
Nel caso di archiviazione dei dati nel pubblico interesse, di ricerca scientifica, storica o a fini statistici, per le quali sono richiesti tempi di conservazione particolarmente lunghi, **è necessario attuare misure tecniche e organizzative adeguate.**



Esattezza dei dati

I dati personali raccolti devono essere **esatti** e **aggiornati**.

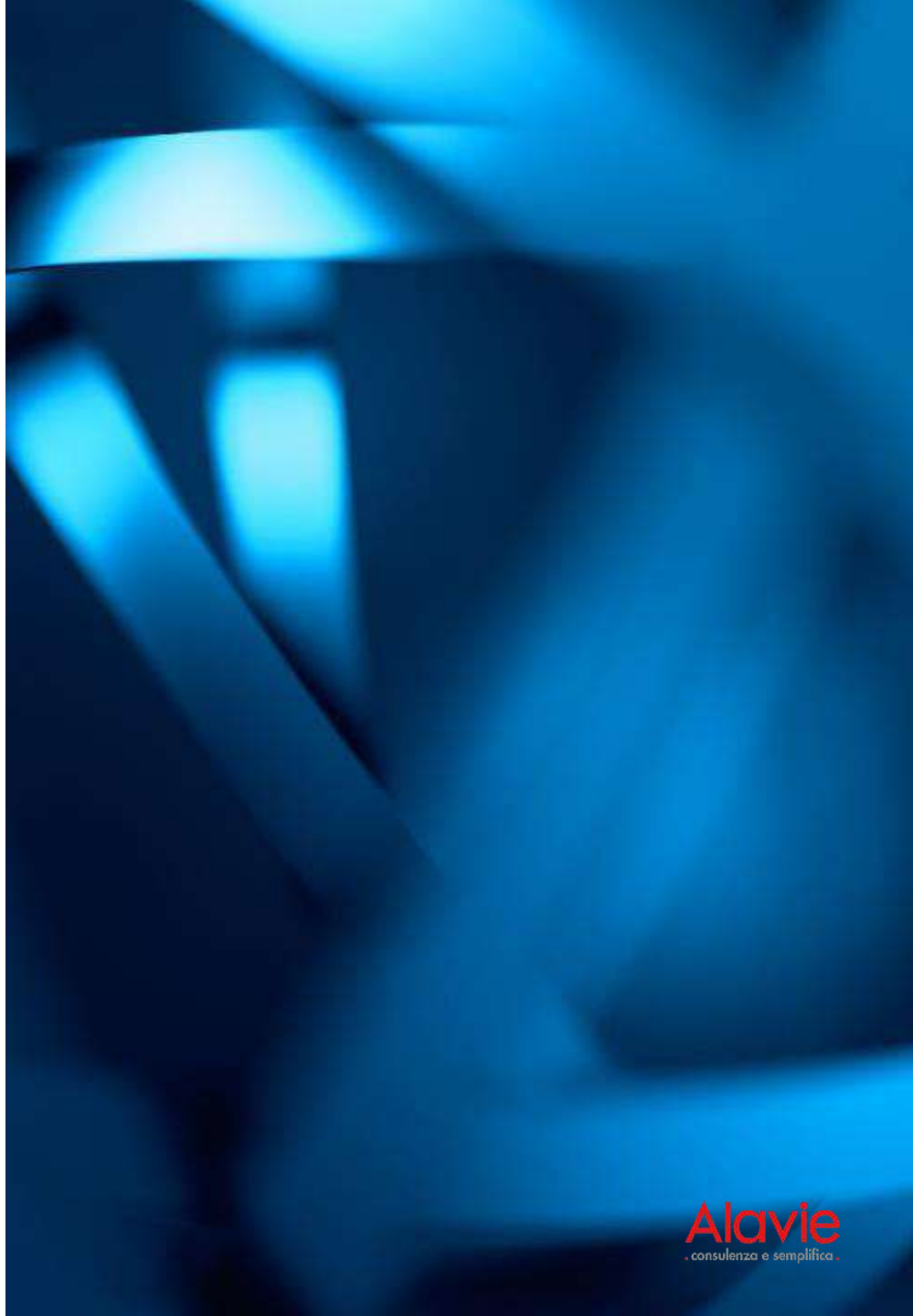
È necessario adottare tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati



Liceità e correttezza

L’uso dei dati può considerarsi lecito se vengono rispettate tutte le norme a protezione dei dati personali.

Il principio di correttezza impone che i dati personali vengano trattati nel rispetto dei principi di lealtà e buona fede.



Garantire sicurezza, riservatezza, integrità e disponibilità

SICUREZZA: adottare misure tecniche e organizzative adeguate

RISERVATEZZA: evitare intercettazione e la lettura da parte di persone non autorizzate

INTEGRITÀ: assicurare che i dati siano completi e inalterati

DISPONIBILITÀ: accessibilità anche in caso di interruzioni dovute a eventi eccezionali o ad attacchi di pirateria informatica.

Profilazione

Qualsiasi forma di **trattamento automatizzato** di dati personali consistente nell'utilizzo di tali dati personali per **valutare determinati aspetti personali relativi a una persona fisica**, viene effettuata per **analizzare** o **prevedere**, ad esempio il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, ecc.

Esempio: i cookie che permettono ai siti web e ai motori di ricerca di tracciare le nostre ricerche, preferenze e gusti per proporre prodotti o servizi

È possibile opporsi ai sistemi automatizzati?

Esempi:

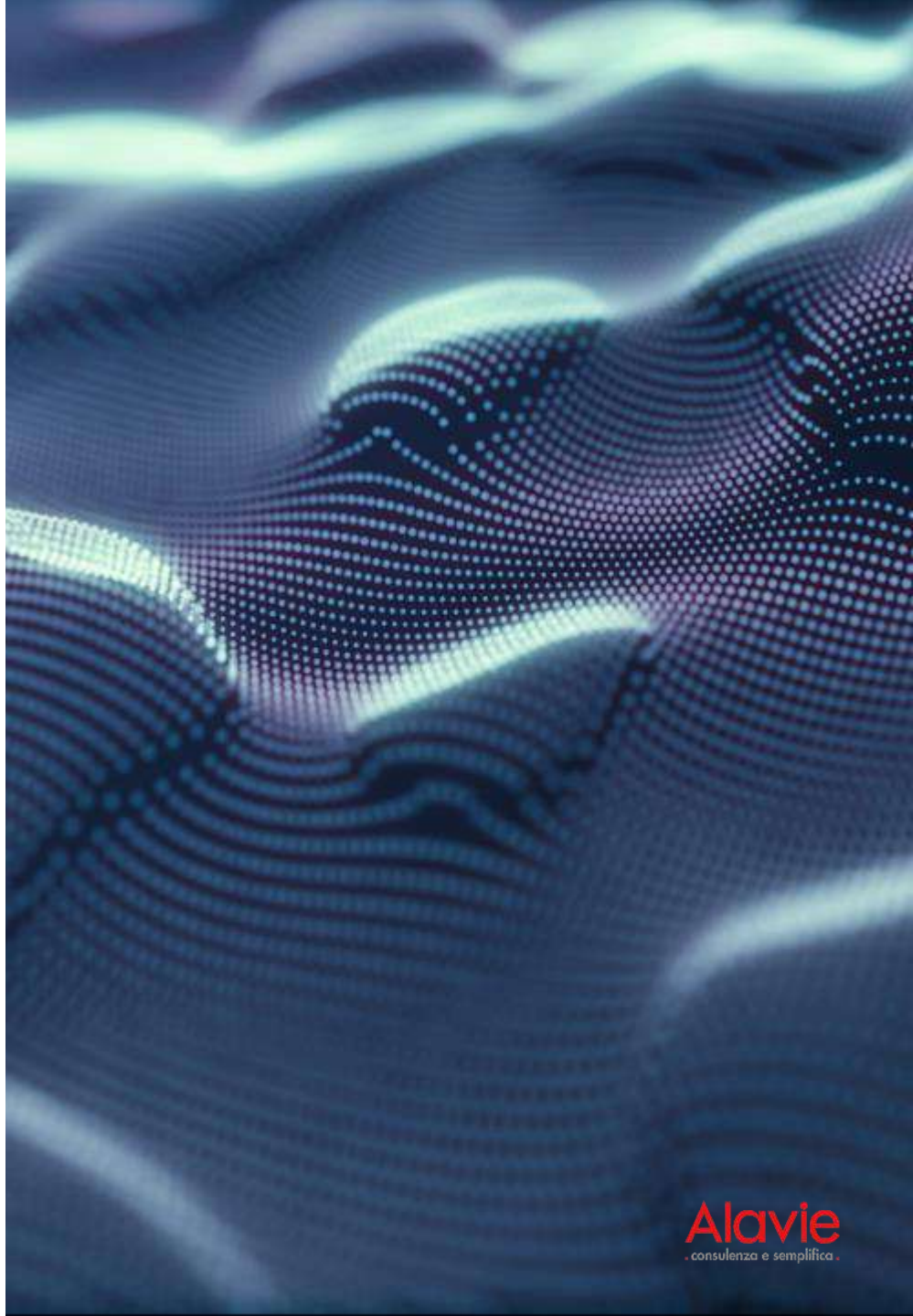
- **Autovelox / Safety tutor**
- **Consenso sito web**
- **Consenso telefono**

E’ possibile opporsi facendo valere in giudizio il legittimo interesse

Alavie
consulenza e semplifica

Contenuti del corso

1. Dal D.Lgs 196/2003 al Regolamento UE 2016/679
2. Le figure del Regolamento UE 2016/679
3. Tipologie di dati ed il loro trattamento
4. Principi chiave del trattamento dei dati
5. **Obblighi del titolare del trattamento**
6. Vademecum e impianto sanzionatorio



Obblighi del titolare del trattamento

Con riferimento al Trattamento dei dati il Legislatore UE richiede che **l'INFORMATIVA Art. 13 GDPR** all'interessato sia:

Linguaggio semplice e chiaro

Elementi

- Finalità del
- Trattamento
- Natura dei dati trattati
- Base giuridica
- Periodo di conservazione
- Diritti dell'interessato
- Destinatari
- Diritto di reclamo all'autorità di controllo
- Eventuale trasferimento dei dati in paesi terzi

Forma Scritta

la forma orale è ammessa solo quando possa essere in ogni caso comprovata con altri mezzi l'identità dell'interessato

Alavie
consulenza e semplifica

Obblighi del titolare del trattamento

Non occorre informare l'interessato quando:

- L'interessato dispone già delle informazioni;
- Comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato;
- L'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'unione o dello stato membro cui è soggetto il titolare;
- I dati personali debbano rimanere riservati per obbligo di segreto professionale disciplinato dal diritto dell'unione o degli stati membri.

Diritti più ampi riconosciuti all’interessato

- **Accesso**: Art. 15 GDPR
- **Cancellazione limitazione**: Art. 16-17-18 GDPR
- **Portabilità dei dati**: Art. 20 GDPR

Cosa cambia in riferimento a questi diritti?

Accesso

E' fondamentale indicare

- Il periodo di conservazione dei dati previsto
- Garanzie applicate in caso di trasferimento dei dati verso paesi terzi.

Oblio

Obbligo di informare della richiesta di cancellazione gli altri titolari che trattino gli stessi dati.
E' esercitabile anche dopo la revoca del consenso

Limitazione

Oltre che in caso di illiceità del trattamento, anche quando l'interessato chieda la rettifica dei dati o si opponga al loro trattamento.

Portabilità

Applicabile ai soli trattamenti automatizzati.
Valido solo per i dati forniti direttamente dall'interessato o sulla
base di un contratto stipulato con questi.
Capacità del titolare di trasferire i dati ad altro titolare su richiesta dell'interessato

Alavie
consulenza e semplifica

La privacy per gli Studi professionali

La documentazione e le prassi di Studio

Art. 30 GDPR

Il registro delle attività di trattamento

Ogni Titolare del Trattamento e, ove applicabile il suo Rappresentante, tengono un Registro delle attività svolte sotto la propria responsabilità.

È obbligatorio per:

- Aziende 250 dipendenti
- Trattamento dati sensibili
- Trattamento dati giudiziari

Il Registro delle attività prevede la mappatura dei trattamenti precisando per ciascuno di essi l'origine e la natura dei dati, le modalità e le finalità di trattamento, i tempi di conservazione, la loro eventuale comunicazione a soggetti terzi, le categorie di interessati, e una descrizione generale delle misure di sicurezza per ciascuna macro area.

Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Alavie
consulenza e semplifica

Il registro dei trattamenti

Art. 30 GDPR

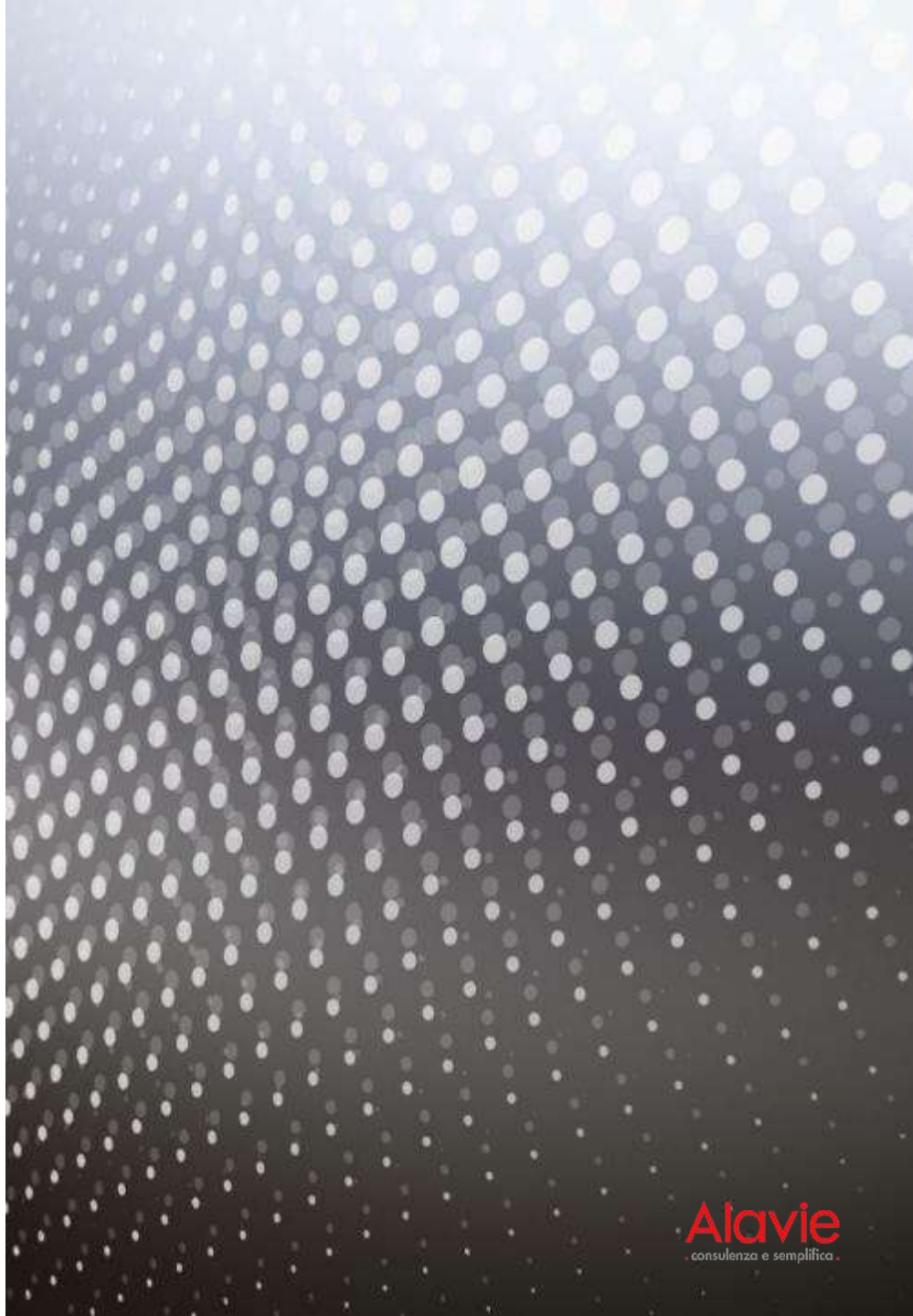
Il registro delle attività di trattamento

Chi deve averlo?

Qualsivoglia persona giuridica che effettui trattamenti continuativi

Esempi:

- Consulenza
- Contabilità



Il registro dei trattamenti

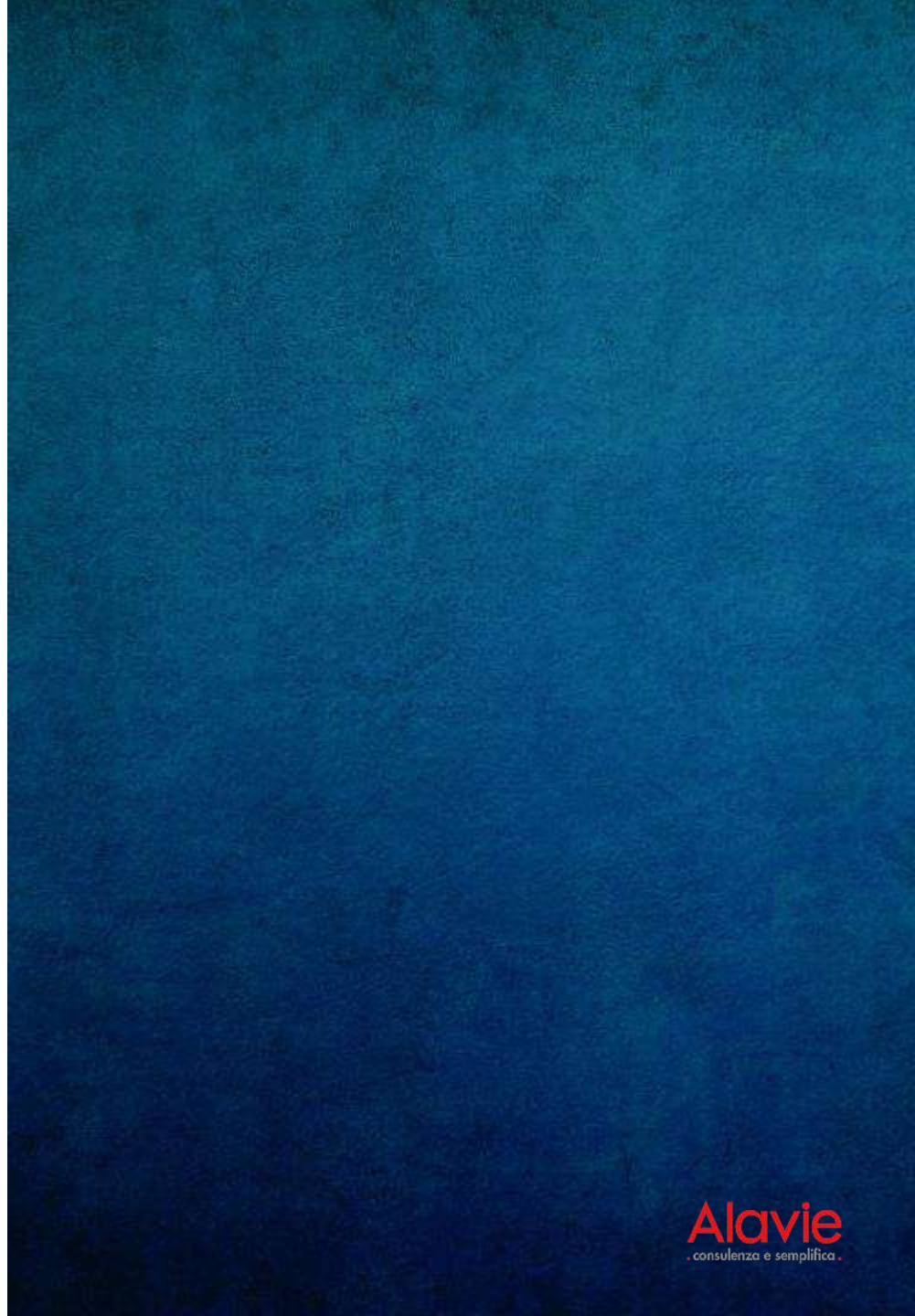
Art. 30 GDPR

Il registro delle attività di trattamento

L'obbligo di redigere il Registro riguarda i titolari o responsabili del trattamento con queste caratteristiche:

- Chiunque effettui trattamenti che possano presentare un rischio, anche non elevato, per i diritti e le libertà dell'interessato;
- Chiunque effettui trattamenti non occasionali;
- Chiunque effettui trattamenti delle categorie particolari di dati o di dati personali relativi a condanne penali e a reati;
- Chiunque abbia almeno 250 dipendenti.

È quindi chiaro che sono obbligati a tenere e redigere il registro dei trattamenti dei dati personali buona parte di imprese e professionisti.
Anche i responsabili del trattamento devono tenere il registro.



Il registro dei trattamenti

FAQ sul registro delle attività di trattamento – Garante Privacy

Alla luce di quanto detto sopra, sono tenuti all'obbligo di redazione del registro, ad esempio:

a) **esercizi commerciali, esercizi pubblici o artigiani con almeno un dipendente** (bar, ristoranti, officine, negozi, piccola distribuzione, ecc.) e/o che trattino dati sanitari dei clienti (es. parrucchieri, estetisti, ottici, odontotecnici, tatuatori ecc.);

b) **liberi professionisti con almeno un dipendente e/o che trattino dati sanitari e/o dati relativi a condanne penali o reati** (es. commercialisti, notai, avvocati, osteopati, fisioterapisti, farmacisti, medici in generale);

c) **associazioni, fondazioni e comitati ove trattino "categorie particolari di dati" e/o dati relativi a condanne penali o reati** (i.e. organizzazioni di tendenza; associazioni a tutela di soggetti c.d. "vulnerabili" quali ad esempio malati, persone con disabilità, ex detenuti ecc.; associazioni che perseguono finalità di prevenzione e contrasto delle discriminazioni di genere, razziali, basate sull'orientamento sessuale, politico o religioso ecc.; associazioni sportive con riferimento ai dati sanitari trattati; partiti e movimenti politici; sindacati; associazioni e movimenti a carattere religioso);

d) **il condominio ove tratti "categorie particolari di dati"** (es. delibere per interventi volti al superamento e all'abbattimento delle barriere architettoniche ai sensi della L. n. 13/1989; richieste di risarcimento danni comprensive di spese mediche relativi a sinistri avvenuti all'interno dei locali condominiali).

Alavie
consulenza e semplifica

Il registro dei trattamenti del Titolare

Cosa deve contenere?

Nome e dati di contatto
titolare, responsabile, rappresentante e RPD

Finalità
del trattamento

Finalità
del trattamento

Trasferimenti all'estero
verso un'organizzazione internazionale, con le adeguate garanzie

Descrizione generale
misure di sicurezza tecniche e organizzative

Termini ultimi
previsti per la cancellazione dei dati

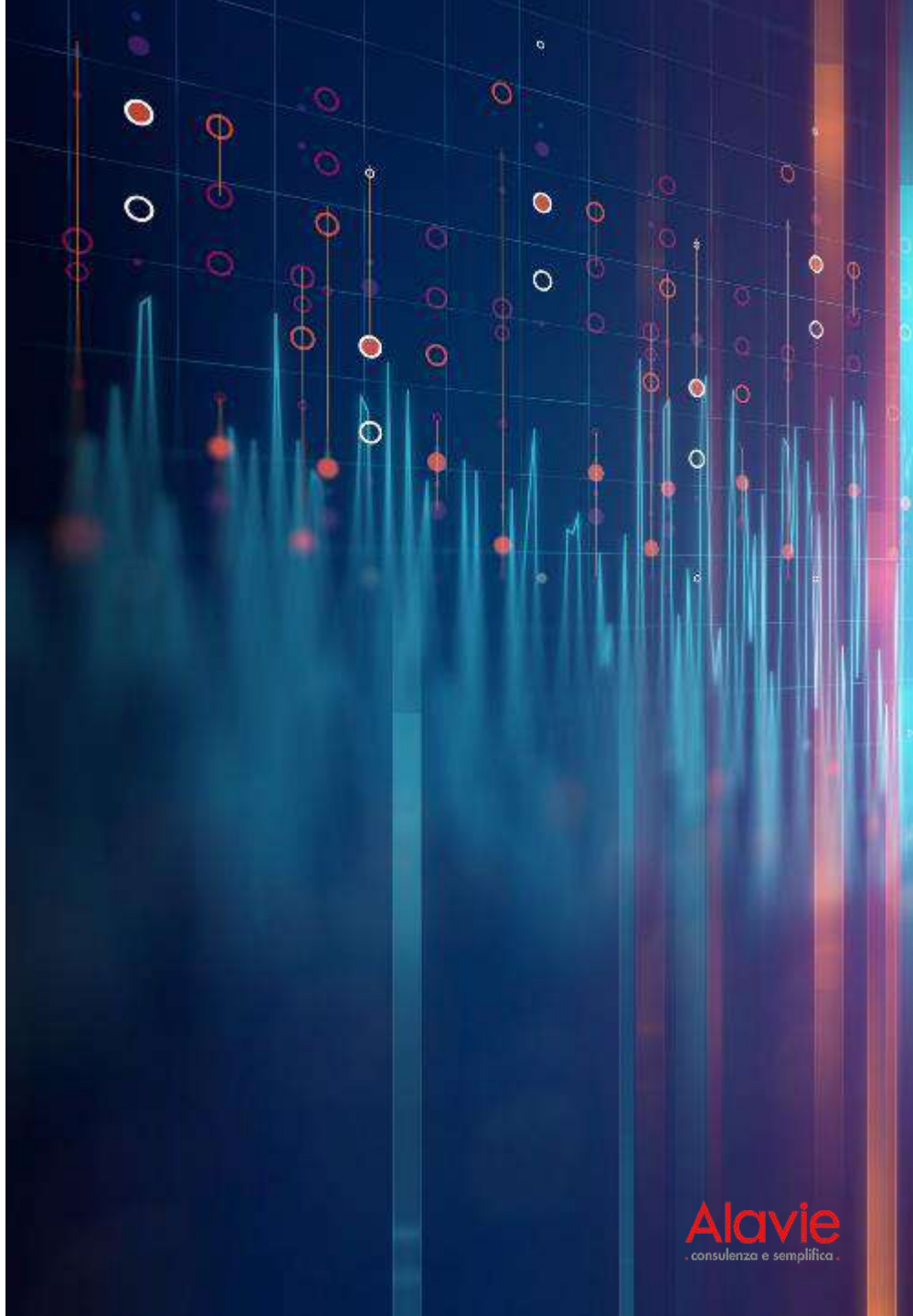
Alavie
consulenza e semplifica

Il registro dei trattamenti

Per le attività svolte ex art. 28 del GDPR

ci si dovrà munire anche di un Registro dei trattamenti

in qualità di Responsabile Esterno



Il registro dei trattamenti del Responsabile Esterno

Cosa deve contenere?

Nome e dati di contatto
titolare, responsabile, rappresentante e RPD

Finalità
del trattamento

Categorie
di interessati e di dati personali trattati

Trasferimenti all'estero
verso un'organizzazione internazionale, con le adeguate garanzie

Descrizione generale
misure di sicurezza tecniche e organizzative

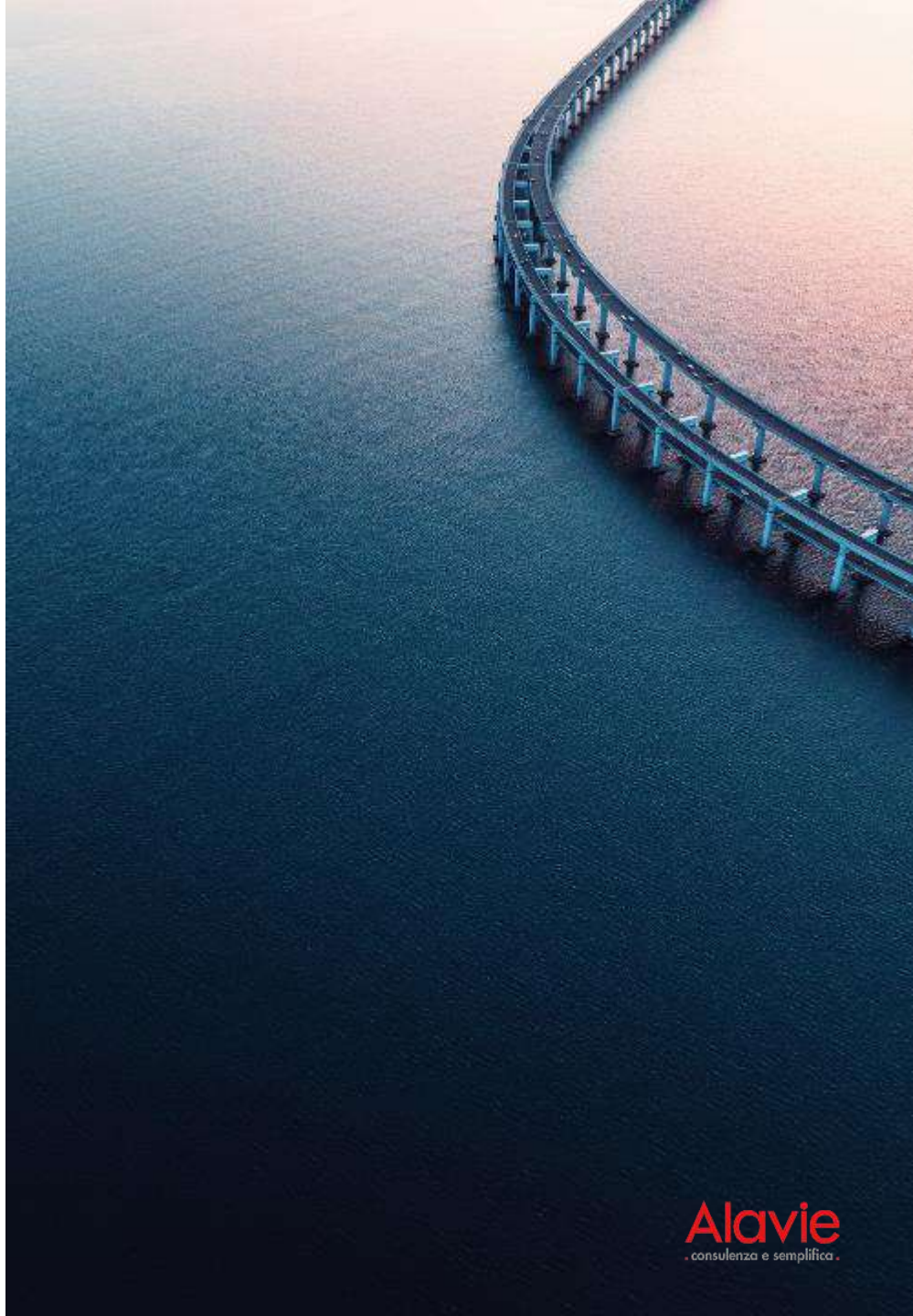
Termini ultimi
previsti per la cancellazione dei dati

Alavie
consulenza e semplifica

I contratti di nomina

Dovranno essere adottati almeno:

- nomina degli autorizzati;
- nomina dei responsabili;
- accordo tra contitolari;
- (eventuale) nomina DPO, con comunicazione al Garante.



Valutazione d’impatto sulla protezione dei dati

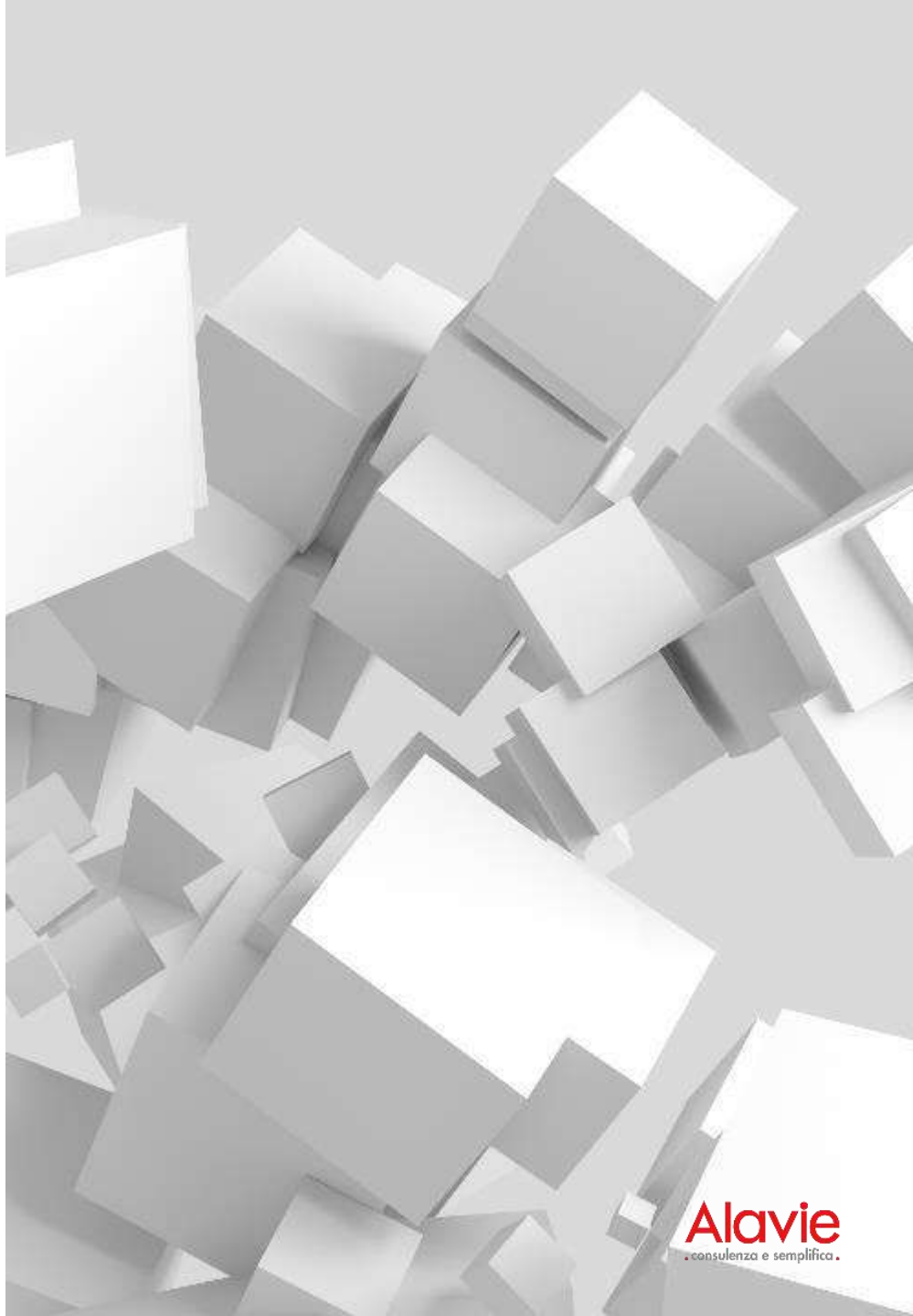
Art. 35 GDPR

Procedura volta alla descrizione di un trattamento per valutarne la necessità e la proporzionalità nonché i relativi rischi

Scelta consapevole ed informata delle misure idonee ad affrontarli

Responsabile della DPIA è il titolare che dovrebbe condurla **prima** di procedere al trattamento.

E’ uno strumento di accountability in quanto è prova di impegno e garanzia da parte del titolare



Cosa indica la valutazione di impatto?

Descrizione sistematica dei trattamenti /delle finalità/ dell'interesse del Titolare

Necessità e proporzionalità dei trattamenti in relazione alle finalità

Valutazione dei rischi per le libertà e i diritti degli interessati

Misure di contrasto al rischio e garanzie

NB. La valutazione d'impatto non costituisce un adempimento una tantum ma è fonte di un onere di **monitoraggio e revisione continui da parte del titolare del trattamento**

Alavie
consulenza e semplifica

D.P.I.A. obbligatoria Art. 35 GDPR

- Valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basato 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;
- Trattamento su larga scala di dati sensibili/ giudiziari;
- Sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Linee guidaWP 29 (4 ottobre 2017):
La D.P.I.A. non è necessaria per i trattamenti che:

- non presentano rischio elevato per diritti e libertà delle persone fisiche;
- hanno natura,, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è
- necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui la definizione è stata condotta una DPIA

Alavie
consulenza e semplifica

Data breach – incidenti di sicurezza dei dati

Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come **la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque trattati.**

Ciò può avvenire a seguito di un attacco informatico, di un accesso abusivo, di un incidente (es. incendio, allagamento, etc.) o per la perdita di un supporto informatico (smartphone, notebook, chiavetta USB, etc.) o per la sottrazione di documenti con dati personali (furto, etc.).
La violazione dei dati personali può essere suddivisa in tre categorie (**R.I.D.**):

a) Violazioni di Riservatezza
b) Violazioni di Integrità
c) Violazioni di Disponibilità

Obbligo di comunicazione al Garante Privacy entro 72 ore dalla scoperta dell'incidente di sicurezza.

Data breach – incidenti di sicurezza dei dati

In generale, notificare entro 72 ore al Garante l'avvenuto data breach

Tranne quando sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche; se la probabilità del rischio per gli interessati è elevata, si dovrà informare delle violazioni anche gli interessati senza ingiustificato ritardo.

Bisognerà quindi:

- mettere in essere procedure standard per il rilevamento e la comunicazione dei data breach;
- valutare il rischio per i diritti e le libertà delle persone;
- tenere traccia delle violazioni e delle valutazioni effettuate;

Obbligo di data breach

Art. 33-34 GDPR

Lo scopo è quello, in caso di violazione , di permettere all'Autorità di controllo di attivarsi senza ritardo in modo da valutare la gravità della violazione e la tipologia di misure da imporre al Titolare.

Responsabile > Titolare > Autorità di controllo

- Natura della violazione
- Natura dei dati
- Numero di interessati
- Nome e contatto del Resp. o di altro referente
- Descrizione delle probabili conseguenze

Entro massimo 72 ore

Conseguenza della violazione

Caso A

Rischio elevato per i diritti e le libertà delle persone fisiche

Comunicazione all'interessato
In termini chiari/ fruibili

Caso B

- il titolare del trattamento ha messo in atto le misure tecniche ed organizzative necessarie alla protezione dei dati violati (es. la cifratura)
- adozione di misure atte a scongiurare il sopraggiungere di un rischio elevato per diritti e libertà dell'interessato
- la comunicazione al singolo interessato risulterebbe troppo gravosa = **comunicazione pubblica**

Non si procede alla comunicazione All'interessato

Alavie
consulenza e semplifica

La violazione dei dati personali

Alavie
consulenza e semplifica

La violazione dei dati personali

Alavie
consulenza e semplifica

La violazione dei dati personali

Violazioni di disponibilità:

- Perdita
- Attacchi informatici
- Malfunzionamenti software con perdita dati
- Guasti hardware
- Inefficacia del backup
- Indisponibilità data center
- Errori operativi
- Interruzione connettività

Misure di sicurezza adeguate (Art. 32)

Non sono più previste misure minime come quelle indicate tassativamente e «tipizzate» nell'allegato B D.Lgs. 196/03

Titolare e responsabile del trattamento

Mettono in atto

Misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio

Tenuto conto dello stato dell'arte e dei costi di attuazione, nonché **natura, ambito, contesto, finalità e rischi**

Misure di sicurezza tipizzate (Art. 32)

- Pseudonimizzazione
- Cifratura
- Capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
- Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento

La formazione

Non si è ottemperanti alla normativa se non si effettua la corretta formazione, anche dei dipendenti e dei collaboratori.

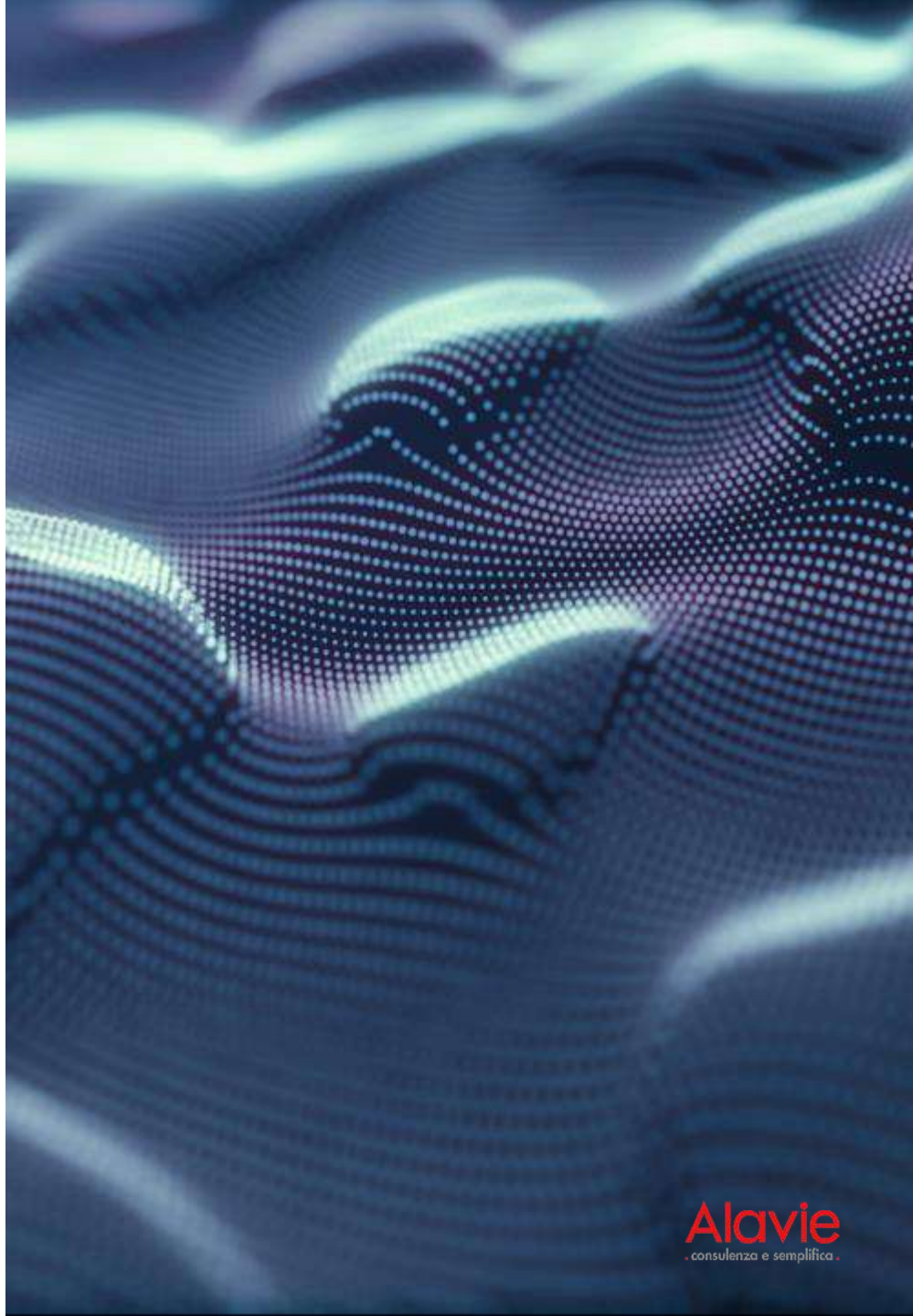
Attenzione:

Come già ricordato, per la «nomina» dei responsabili e degli autorizzati al trattamento bisognerà verificare anche questo aspetto.

«L' 'antivirus' del fattore umano è la formazione»

Contenuti del corso

1. Dal D.Lgs 196/2003 al Regolamento UE 2016/679
2. Le figure del Regolamento UE 2016/679
3. Tipologie di dati ed il loro trattamento
4. Principi chiave del trattamento dei dati
5. Obblighi del titolare del trattamento
6. **Vademecum e impianto sanzionatorio**



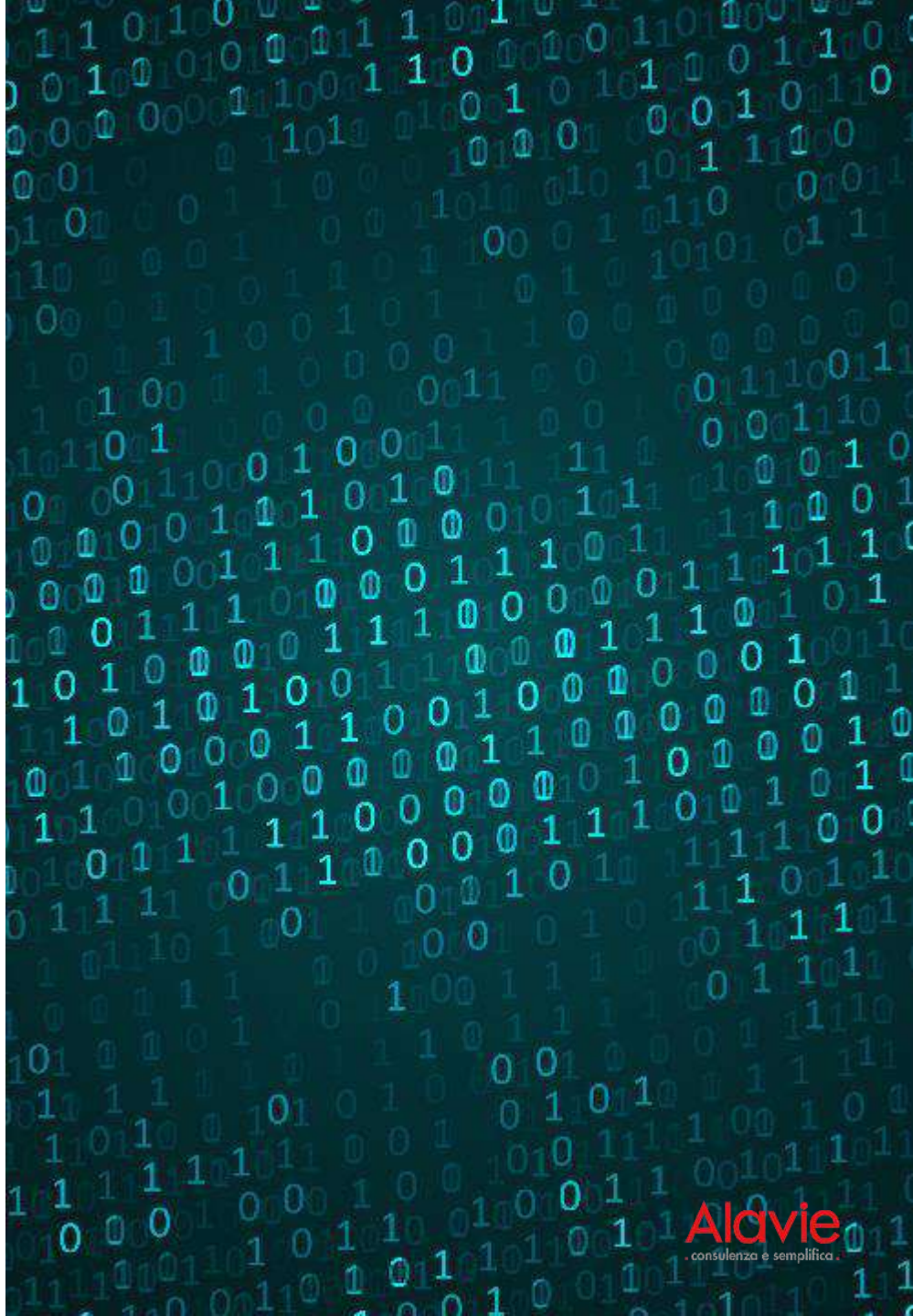
Vademecum per evitare violazioni

- Conoscere le regole sulla protezione dei dati personali ed i rischi
- Pensare prima di agire
- Non divulgare a terzi estranei le informazioni di cui si viene a conoscenza in ambito lavorativo
- Adoperarsi affinché terzi fraudolentemente non entrino in possesso di dati raccolti
- Non fare copie, per uso personale, dei dati su cui si opera in azienda

Vademecum per evitare violazioni

- Trattare i dati in modo lecito e secondo correttezza e per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti;

- Attenersi scrupolosamente alle istruzioni scritte impartite dal Titolare del trattamento, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme



Vademecum per evitare violazioni

- **Far rispettare le policy aziendali/regolamenti di Studio:**

  - Limitare l’utilizzo di dispositivi aziendali e personali, per i possibili rischi correlati alla protezione delle informazioni e dei dati personali.
  - adottare un approccio proattivo alla sicurezza delle informazioni e alla gestione dei dati personali.

Vademecum per evitare violazioni

La maggioranza degli attacchi informatici e di fughe di dati

Accadono **a causa di un errore o di un comportamento doloso**

da parte dei dipendenti !

Anche il mancato rispetto della privacy è dovuto spesso ad **errori umani**.

Il mancato rispetto della legge è soggetto a **pesanti sanzioni**.

Nuove prassi da adottare

Tenendo conto dello stato dell'arte e dei **costi di attuazione**, nonché della natura e del rischio per i diritti e le libertà delle persone fisiche, bisognerà porre in atto misure tecniche e organizzative adeguate, ad esempio:

- La pseudonimizzazione e la cifratura dei dati personali;
- Backup tali da assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi;
- Prassi volte a ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico;
- Bisognerà periodicamente testare l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nuove prassi da adottare

I gestionali di studio e le configurazioni di rete (es. firewall) dovranno garantire, ad esempio:

- La tracciabilità dei log, cioè gli accessi dovranno essere personali, monitorabili;
- Che ogni utente (es. dipendente, collaboratore) possa vedere, trattare solo i dati per i quali è autorizzato;
- Che tutti gli accessi da remoto avvengano da e per una rete sicura e cifrata.

Alavie
consulenza e semplifica

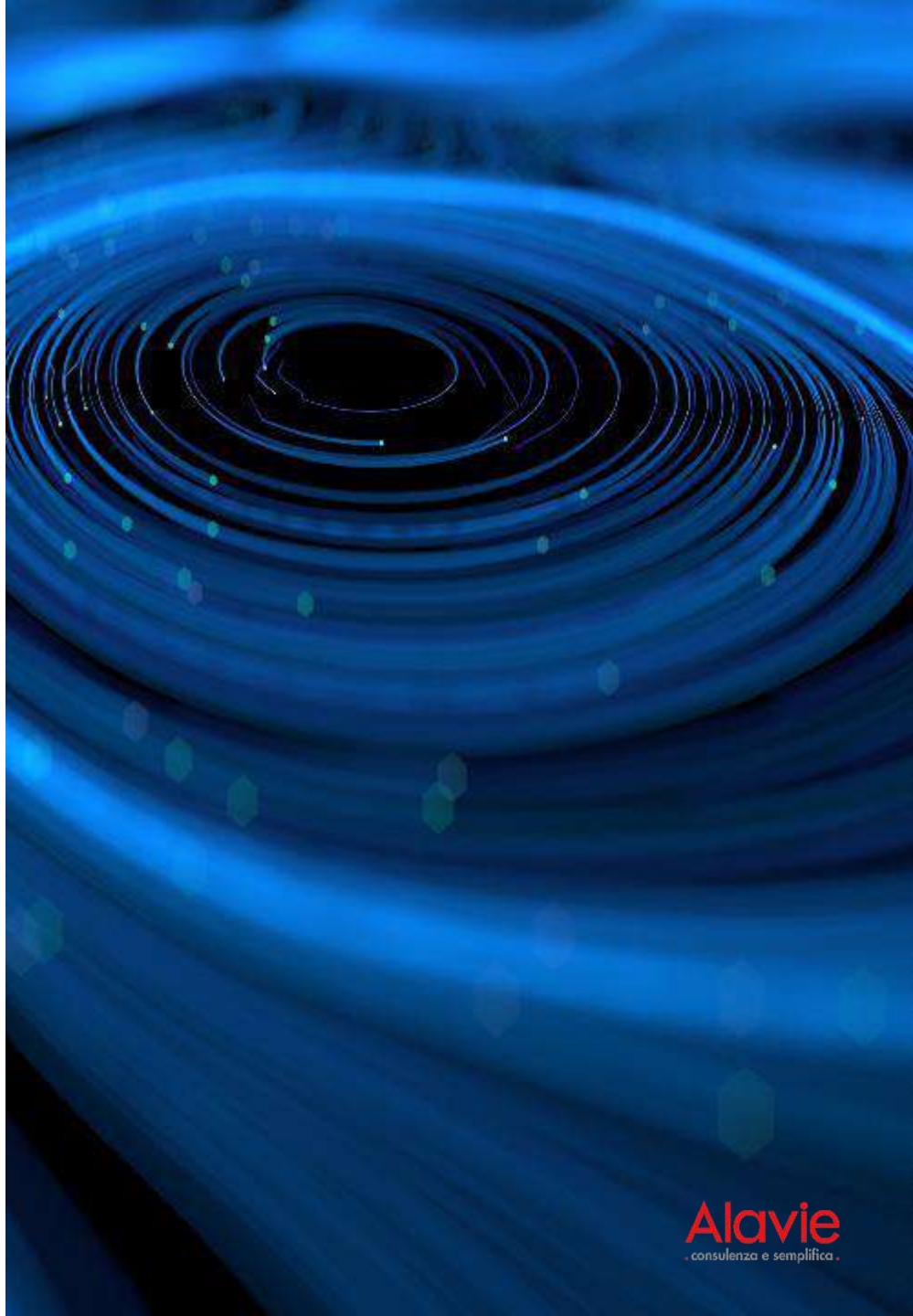
Nuove prassi da adottare

Non limitiamoci alla parte informatica, ad esempio:

- Lo studio dovrà essere messo in sicurezza (per quanto possibile) da furti ed accessi non autorizzati;
- Gli armadi con i documenti cartacei non devono essere accessibili ai non autorizzati;
- Le scrivanie e gli schermi dovranno essere orientati correttamente;
- Lo studio dovrà essere dotato di distruggidocumenti a norma;
- Anche i documenti cartacei andranno pseudonimizzati;
- Le fotocopiatrici, i fax e le stampati dovranno essere a norma;
- Anche le imprese di pulizie sono un rischio da calcolare.

Opportunità e spunti di riflessione

- Modernizzare e digitalizzare gli studi e, soprattutto, i processi, i flussi dei dati;
- Più sicurezza e più garanzie di continuità degli studi professionali;
- Nuove specializzazioni es. DPO e/o consulente privacy;
- Nuove possibilità per i formatori;
- Impatto su collegi sindacali e continuità aziendale;
- Nuove forme di certificazione delle competenze in tema privacy.



Ispezioni: come avvengono?

Motu proprio/su iniziativa del garante

A seguito di segnalazione dell'interessato

Annunciate

Di sorpresa

Come si concludono?

- Accountability
- Provvedimenti correttivi
- Sanzioni

Alavie
consulenza e semplifica

L’impianto sanzionatorio

GDPR & D. Lgs 101/2018 a confronto

Regolamento UE 2016/679 – sanzioni amministrative

Fino a 20 mln € o fino al 4% del fatturato per le seguenti violazioni:

- Inosservanza di un ordine o limitazione al trattamenti imposti dal Garante Privacy
- Trasferimento illecito di dati fuori dall’UE

Fino a 10 mln € o fino al 2% del fatturato mondiale annuo riferito all’anno precedente per le seguenti violazioni:

- Mancato consenso
- Trattamento illecito dei dati soggetti all’informativa
- Mancata comunicazione della violazione dei dati al Garante Privacy
- Mancata nomina del DPO
- Mancata applicazione delle misure di sicurezza adeguate

Alavie
consulenza e semplifica

L’impianto sanzionatorio

GDPR & D. Lgs 101/2018 a confronto

Decreto Legislativo 101/2018 – sanzioni penali

Reclusione da 1– 6 anni per:
Comunicazione e diffusione illecita di dati personali trattati su larga scala

Reclusione da 1– 4 anni per:
Acquisizione fraudolenta di dati personali su larga scala

Reclusione da 6 mesi – 3 anni per:
Falsità nelle dichiarazioni al Garante

Reclusione da 3 mesi – 2 anni per:
Inosservanza dei provvedimenti del Garante Privacy

Alavie
consulenza e semplifica

L’impianto sanzionatorio

GDPR & D. Lgs 101/2018 a confronto

Reclusione da 6 - 18 mesi per:
Trattamento illecito di dati

Reclusione da 15 giorni – 1 anno oppure ammenda da 154€ - 1549€ per:
Violazione delle disposizioni in materia di controllo a distanza e indagini sulle opinioni dei lavoratori (Statuto dei lavoratori l. 300/1970)

Videosorveglianza (una delle modalità di controllo a distanza)
E' necessario, in alternativa:

- un accordo sindacale
- un’istanza alla Direzione Territoriale del Lavoro

Alavie
consulenza e semplifica

Sanzioni Garante italiano

- **14 GENNAIO 2021: REGIONE LAZIO**

  75 MILA EURO DI SANZIONE -> MANCATA NOMINA EX ART. 28

- **25 MAGGIO 2021: UNIVERSITA' FEDERICO II DI NAPOLI**

  10 MILA EURO DI SANZIONE -> IMPIANTO DI VIDEOSORVEGLIANZA

- **13 LUGLIO 2021: WIND-TRE**

  17 MILIONI DI EURO DI SANZIONE -> ATTIVITA' DI MARKETING ILLEGALE

Alavie

. consulenza e semplifica .

www.alavie.it

contattaci@alavie.it

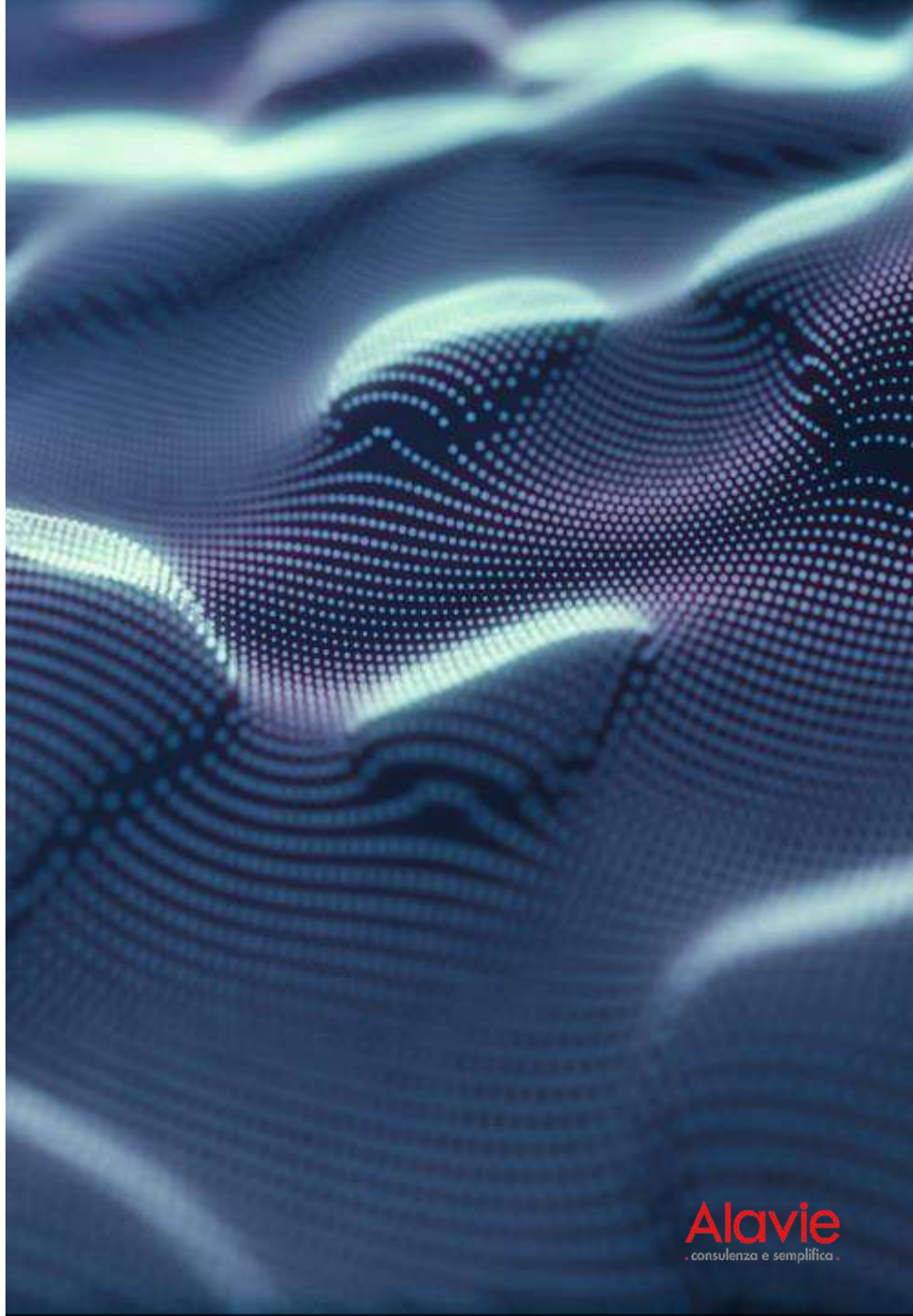
Cyber Security

Webinar ALAVIE

Alavie
. consulenza e semplifica .

Contenuti del modulo Cyber Security

1. **Definizione di Cyber Security**
2. Quadro Normativo Europeo e Nazionale
3. Rischio Cyber Security
4. Attacco Cyber Security
5. Tecniche di Attacco
6. Rapporto CLUSIT 2024
7. Misure di Sicurezza
8. Formazione Cyber Security



Definizione di Cyber Security (1)

- **«Cibersicurezza»**: l'insieme delle **attività** necessarie per **proteggere** la **rete** e i **sistemi informativi**, gli **utenti** di tali sistemi e altre persone interessate dalle minacce informatiche - *Art. 2, punto 1), Regolamento (UE) 2019/881 del 18 gennaio 2019*, relativo alla Cibersicurezza.

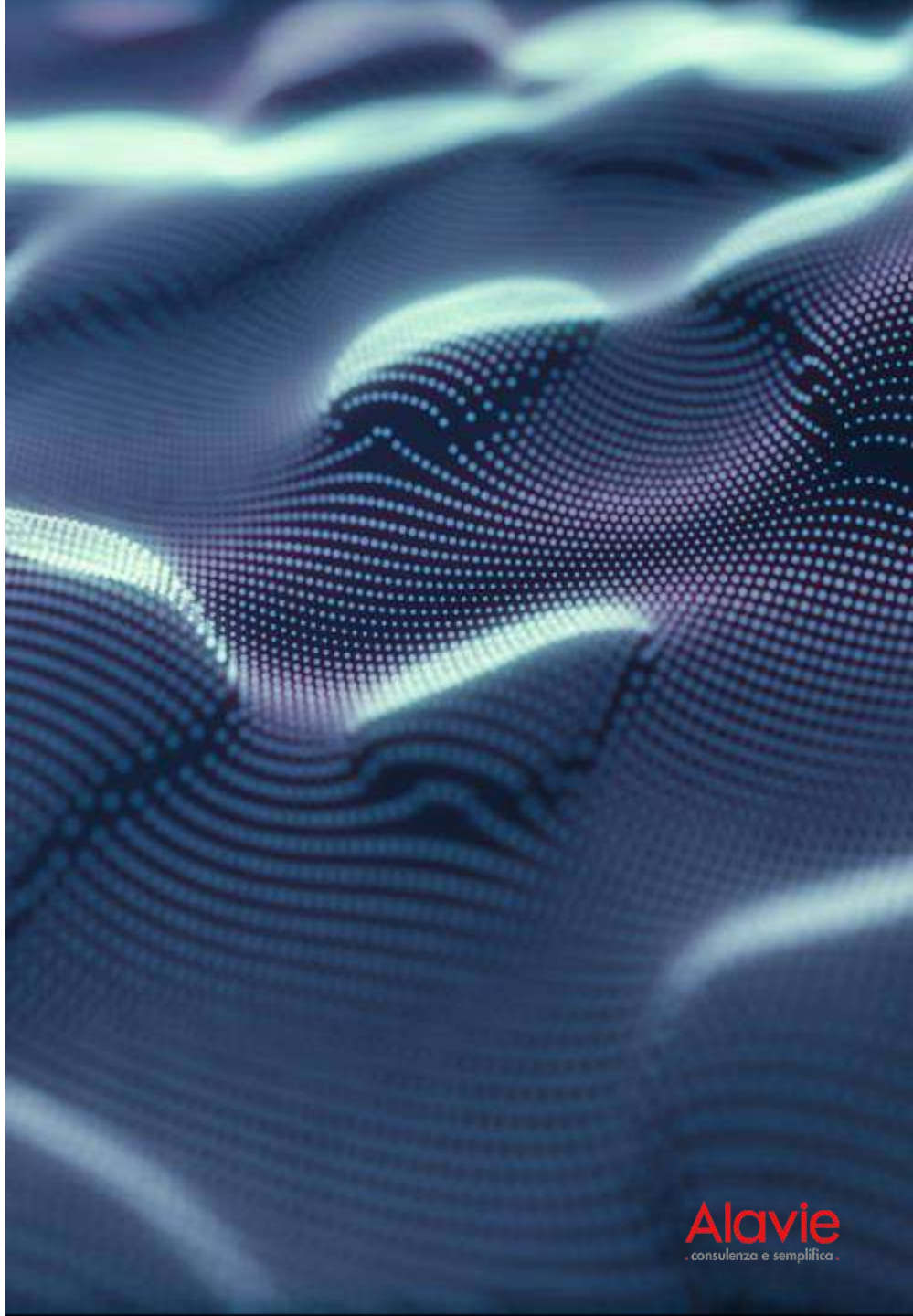
Definizione di Cyber Security (2)

- **«Minaccia informatica»**: qualsiasi **circostanza**, **evento** o **azione** che potrebbe **danneggiare**, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone - *Art. 2, punto 8), Regolamento (UE) 2019/881.*

- La *mission* della **cybersicurezza** è la **protezione della rete, dei sistemi e degli utenti dalle «minacce informatiche».**

Contenuti del modulo Cyber Security

1. Definizione di Cyber Security
2. **Quadro Normativo Europeo e Nazionale**
3. Rischio Cyber Security
4. Attacco Cyber Security
5. Tecniche di Attacco
6. Rapporto CLUSIT 2024
7. Misure di Sicurezza
8. Formazione Cyber Security



La Normativa

Europea

Nazionale

Quadro Normativo Europeo - NIS (1)

- La **Direttiva 2016/1148** (**NIS** - *Network Information System)*, adottata dall'Unione Europea nel 2016 e recepita in Italia dal Decreto Legislativo del 18 maggio 2018, stabilisce i **requisiti minimi per la sicurezza delle reti e dei sistemi informativi nell'UE**.
- Si applica agli operatori di servizi essenziali (OSE) e ai fornitori di servizi digitali (DSP).

Quadro Normativo Europeo - NIS (2)

- **La direttiva NIS si basa su tre pilastri:**

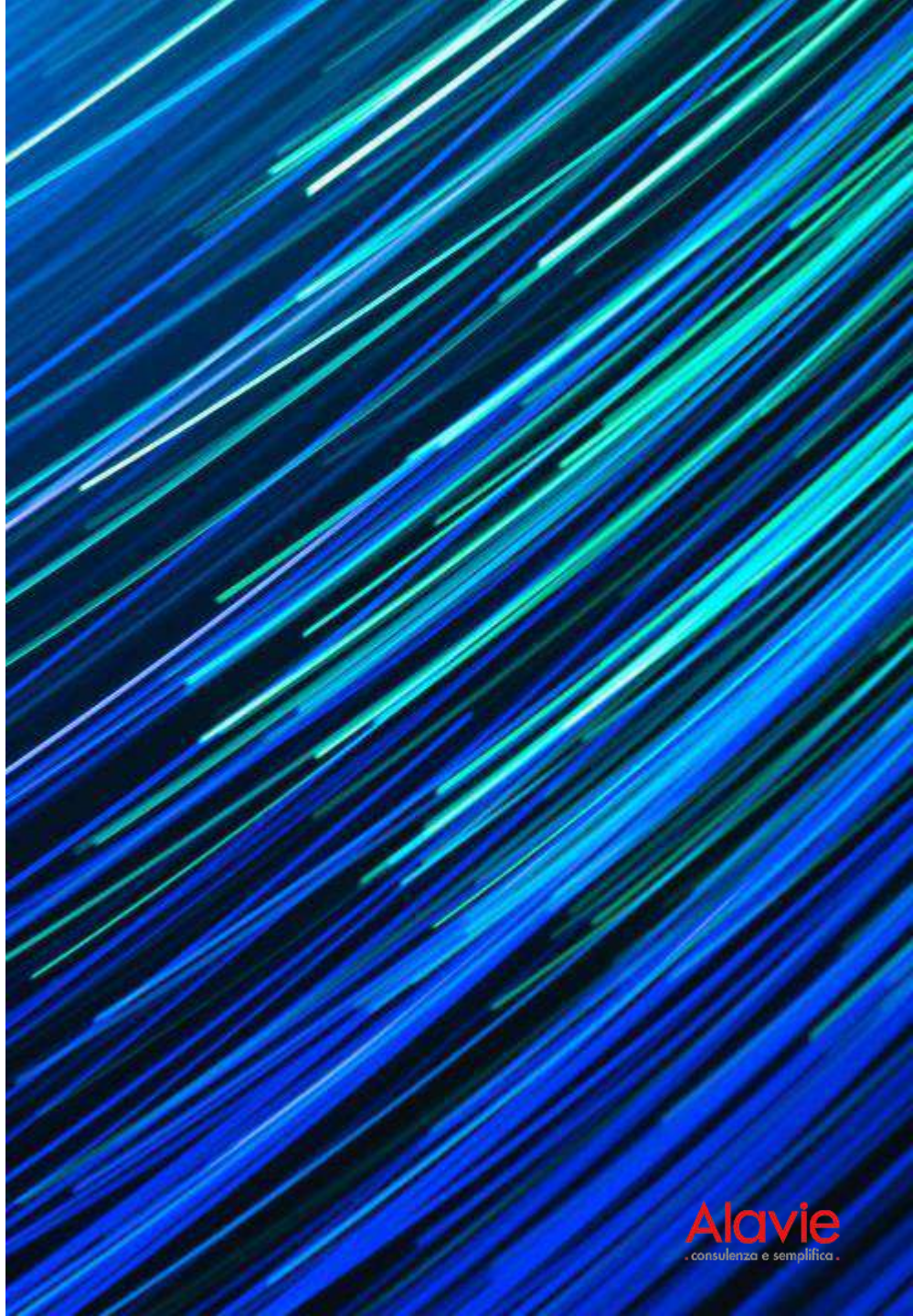
1. **Prevenzione**: gli operatori di servizi essenziali e i fornitori di servizi digitali devono mettere in atto misure per prevenire gli attacchi informatici;
2. **Rilevamento**: gli stessi devono essere in grado di individuare tempestivamente gli attacchi informatici;
3. **Mitigazione**: essi devono essere in grado di ripristinare rapidamente i propri servizi in caso di attacco informatico.

Quadro Normativo Europeo - NIS (3)

- La nuova direttiva NIS2 mira a stabilire una strategia comune di cybersecurity per tutti gli Stati membri, elevando i livelli di sicurezza dei servizi digitali su scala europea. ;
- Elimina la distinzione tra gli operatori di servizi essenziali (OSE) e i fornitori di servizi digitali (DSP), introducendo **nuove categorie di operatori** basate sull'importanza del servizio offerto. Distingue tra i **“soggetti essenziali”** e i **“soggetti importanti”;**

Quadro Normativo Europeo - NIS (4)

- Estende gli obblighi di cybersecurity a un numero maggiore di settori e servizi considerati critici per il funzionamento socioeconomico dell'UE includendo **piattaforme di cloud computing, data center e servizi sanitari.**
- La direttiva stabilisce anche un quadro più dettagliato per le misure di sicurezza, richiedendo **un approccio multirischio** e la segnalazione tempestiva di incidenti significativi alle autorità competenti.



Quadro Normativo Europeo - NIS (5)

- **Cyber e Governance:** la gestione della *cyber* sicurezza non è più un compito relegato esclusivamente alla funzione IT, ma diventa una responsabilità diretta dell'organo di gestione aziendale, come il CDA. Esso provvederà ad approvazione di misure tecniche per la gestione del rischio cyber, alla supervisione e all'implementazione di tali misure e a formarsi specificamente sul tema.
- ART. 21: **MISURE DI GESTIONE DEI RISCHI**: politiche di analisi dei rischi, strategie per la gestione degli incidenti, piani di continuità operativa, sicurezza della catena di approvvigionamento, e pratiche di igiene informatica.

Quadro Normativo Europeo - NIS (6)

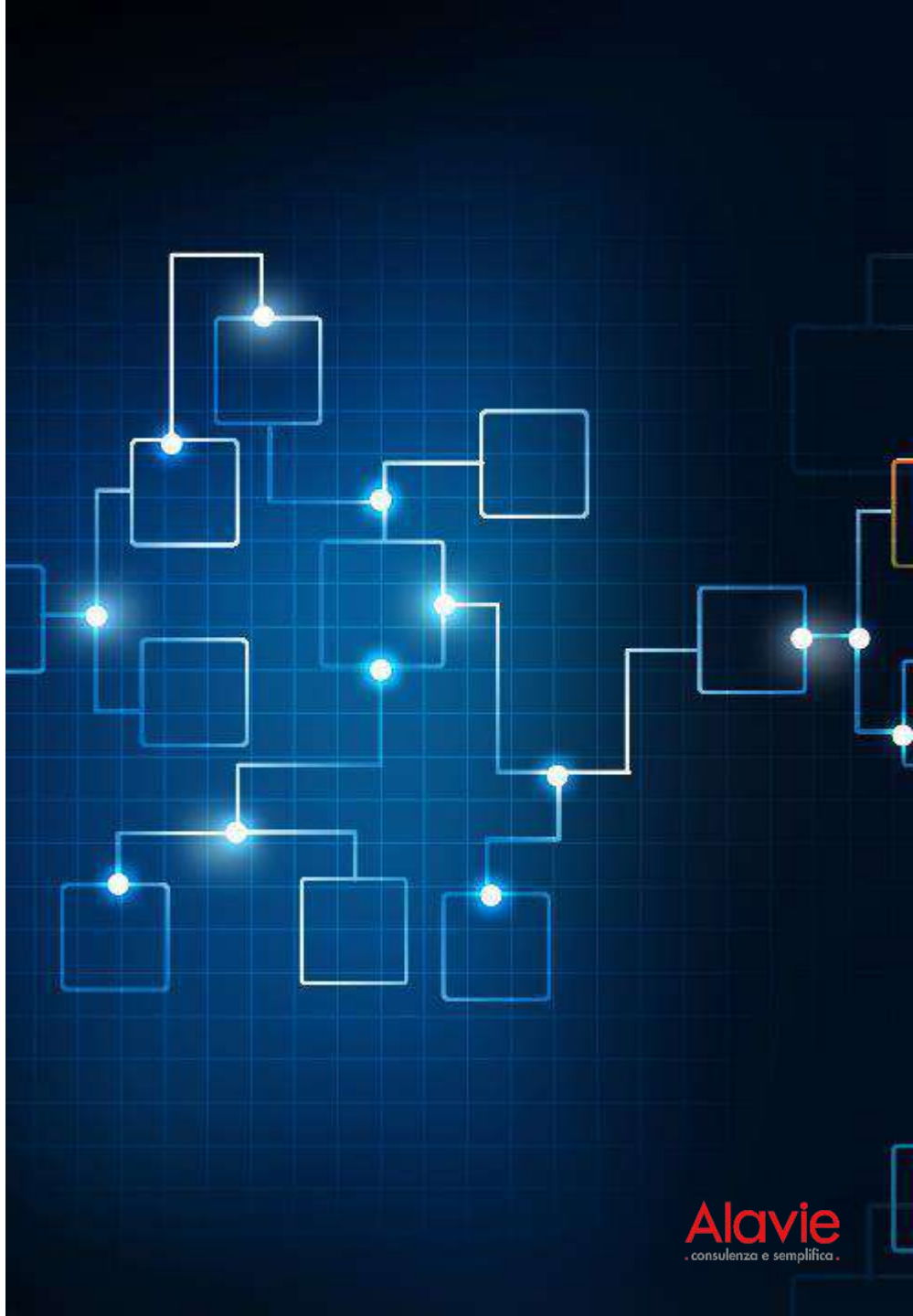
- La Direttiva NIS2 fornisce una definizione più dettagliata di **incidente**: "*un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei relativi servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi*".
- Inoltre, nel nuovo quadro normativo un incidente sarà considerato significativo **anche se ha solo il potenziale di causare un danno**.

Quadro Normativo Europeo – GDPR 2016/679 (1)

- **GDPR 2016/679** – «*General Data Protection Regulation*»
- Principi generali del trattamento di dati personali:
  - **liceità, correttezza e trasparenza** del trattamento, nei confronti dell'interessato;
  - **limitazione della finalità del trattamento**, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;

Quadro Normativo Europeo - GDPR 2016/679 (2)

- Principi generali del trattamento di dati personali:
  - **minimizzazione dei dati**: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
  - **esattezza e aggiornamento dei dati**, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;



Quadro Normativo Europeo - GDPR 2016/679 (3)

- Principi generali del tratt3mento di dati personali:
  - **limitazione della conservazione**: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
  - **integrità e riservatezza**: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Quadro Normativo Europeo CYBERSECURITY ACT 2019/881

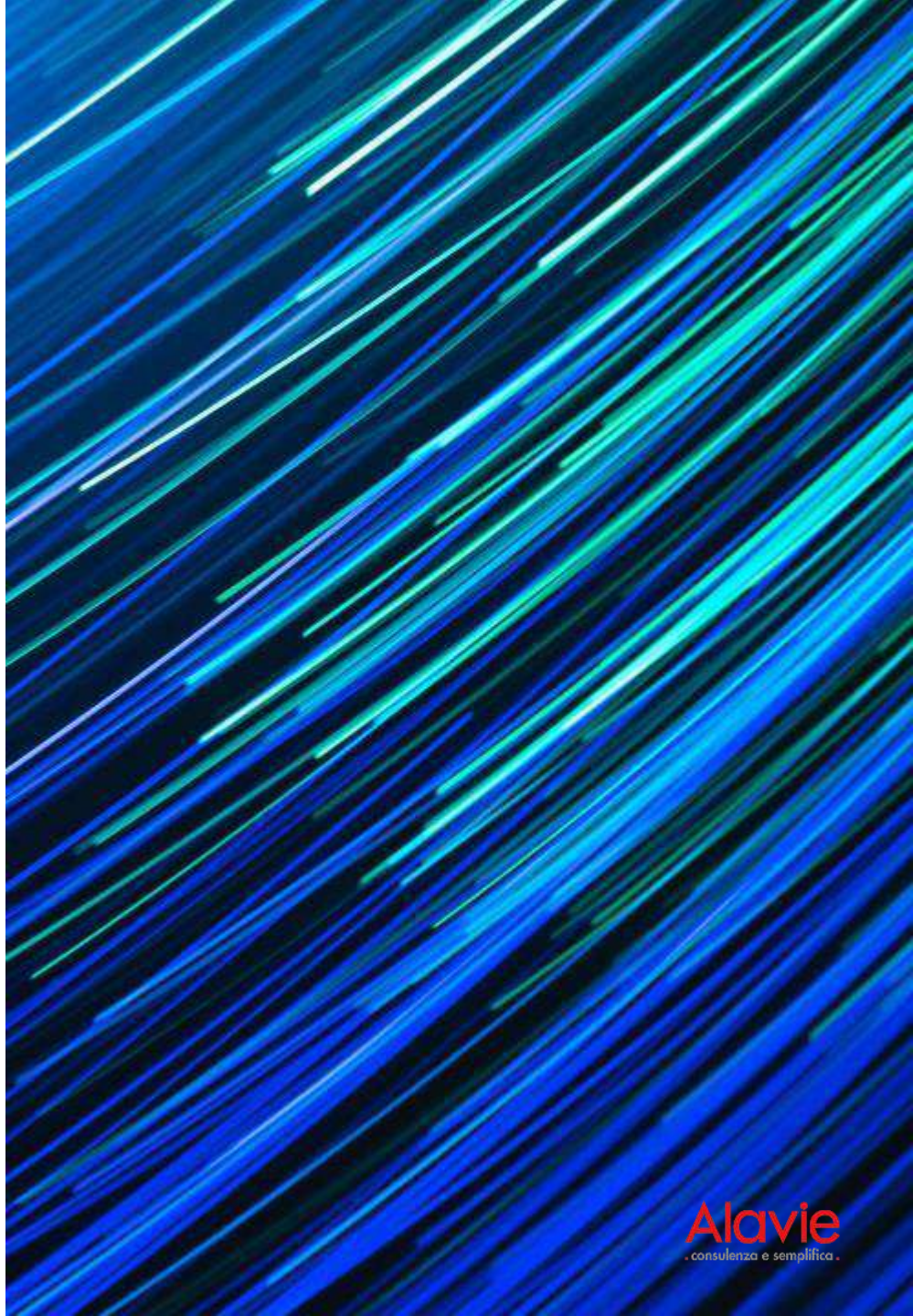
- Il **Regolamento (UE) 2019/881** (***Cybersecurity Act***) è entrato in vigore il 27 giugno 2019.
- Il *Cybersecurity Act* ha un duplice obiettivo:
  1. creare un quadro europeo per la **certificazione** della sicurezza informatica di prodotti ICT e servizi digitali,
  2. rafforzare il **ruolo** dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (**ENISA**).

Quadro Normativo Europeo CYBERSECURITY ACT 2019/881

- Il *Cybersecurity Act* costituisce una parte fondamentale della nuova strategia dell'UE per la sicurezza cibernetica, che mira a rafforzare la resilienza dell'Unione agli attacchi informatici, a creare un mercato unico della sicurezza cibernetica in termini di prodotti, servizi e processi e ad accrescere la fiducia dei consumatori nelle tecnologie digitali.

Quadro Normativo Italiano - DPCM GENTILONI 17 Febbraio 2017

- Sostituisce il DPCM del 24 gennaio 2013 (c.d. Decreto Monti).
- Riorganizza e razionalizza le **risorse** e il **sistema di difesa dello spazio cibernetico nazionale** in linea con le indicazioni menzionate nelle Direttive NIS e NIS2.



Quadro Normativo Italiano - D.LGS 65/2018

- Il **Decreto Legislativo del 18 maggio 2018, n.65** è stato introdotto nel nostro ordinamento in **attuazione della Direttiva 2016/1148 (NIS)** del Parlamento Europeo e del Consiglio recante misure per un livello comune ed elevato di sicurezza delle reti e dei sistemi informativi nell'Unione Europea.

Quadro Normativo Italiano Reg. Perimento Sicurezza

Nazionale Cibernetica 2020/261

- Regolamento in materia di Perimetro di Sicurezza Nazionale Cibernetica 2020/261 – realizzato con il DPCM 131/2020 e definito con il D.L. 105/2019.
- Progetto che si delinea in 5 decreti attuativi volti a definire un quadro normativo di sicurezza nazionale che permetta al sistema paese di entrare in un uovo modello di protezione da minacce Cyber, basato su una continua gestione del rischio.

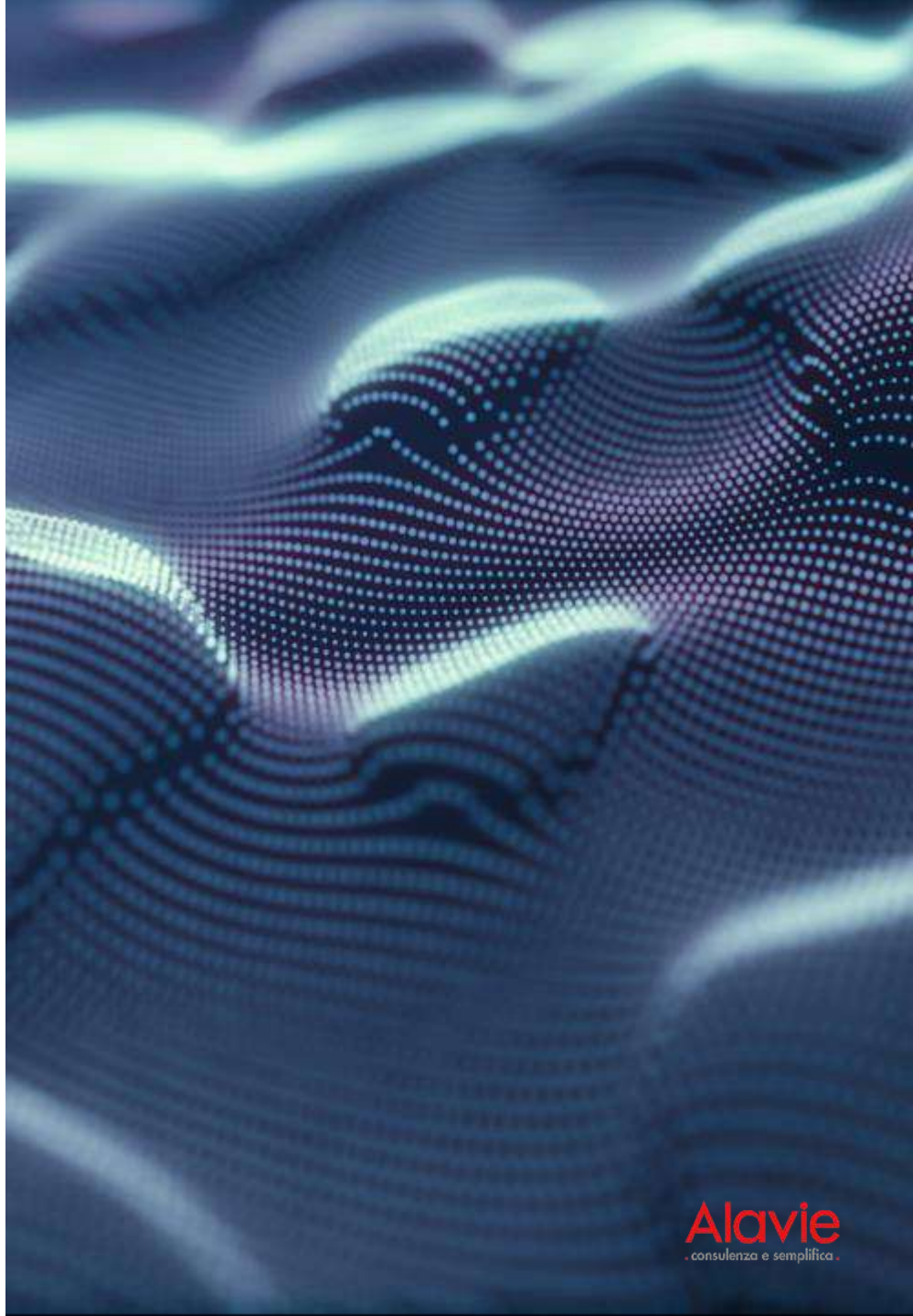
Quadro Normativo Italiano Reg. Perimento Sicurezza

Nazionale Cibernetica 2020/261

- Il **DPCM n. 131/2020** definisce **modalità e criteri procedurali** di individuazione dei soggetti pubblici e privati inclusi nel Perimetro di Sicurezza Nazionale Cibernetica, nonché i criteri attraverso i quali questi soggetti dovranno predisporre e aggiornare un elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza.

Contenuti del modulo Cyber Security

1. Definizione di Cyber Security
2. Quadro Normativo Europeo e Nazionale
3. **Rischio Cyber Security**
4. Attacco Cyber Security
5. Tecniche di Attacco
6. Rapporto CLUSIT 2024
7. Misure di Sicurezza
8. Formazione Cyber Security



Rischio Cyber Security

- OPERATIVO
- FINANZIARIO
- STRATEGICO
- ORGANIZZATIVO
- AZIENDALE

Alavie
consulenza e semplifica

Rischio Cyber Security

FATTORE ORGANIZZATIVO

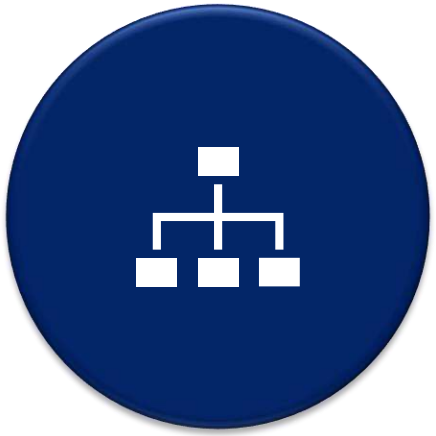
ELEMENTO OGGETTIVO

FATTORE UMANO

ELEMENTO SOGGETTIVO

Alavie
consulenza e semplifica

Rischio Cyber Security – Fattore Organizzativo



Il Titolare è chiamato ad eseguire un duplice ***assessment*** poiché duplice è l'elemento in base al quale varia il rischio cui egli è esposto.

ELEMENTO OGGETTIVO

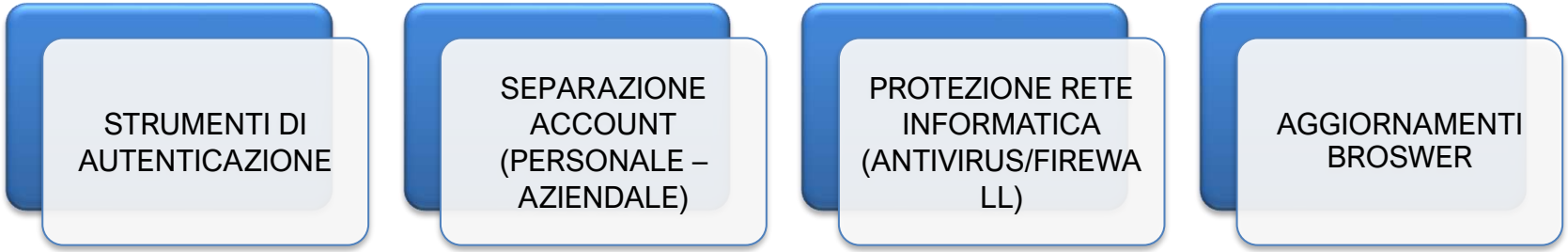
1.1 ELEMENTO OGGETTIVO
INTERNO – Ex art. 32, c. I e II, GDPR

1.2. ELEMENTO OGGETTIVO
ESTERNO – Ex art. 28 GDPR

Alavie
consulenza e semplificazione

1.1 Elemento Oggettivo Interno

Programma di Sicurezza



SICUREZZA da garantire

OBIETTIVI da perseguire

1.2 Elemento Oggettivo Esterno

Gestione della *Supply Chain*

- **Verificare l'adeguatezza e la conformità** rispetto ai prinicipi di cui all'*art.5 del Regolamento Europeo 2016/679* da parte dei responsabili esterni del trattamento (detti altresì fornitori).
- L'assunto è sancito all'*art. 28 del GDPR*, dove il titolare del trattamento è espressamente obbligato a procedere con una valutazione di adeguatezza dei responsabili del trattamento (si legga anche, dei fornitori) che trattano dati personali per suo conto.
- Tale valutazione non può escludere gli **aspetti di sicurezza informatica** offerti o richiesti.

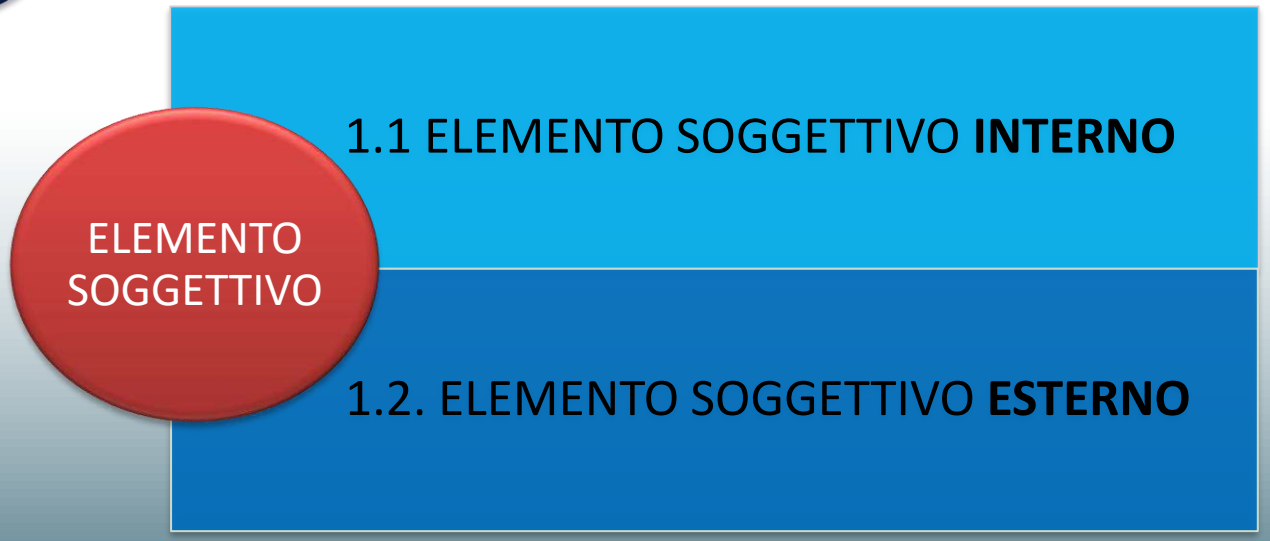
Alavie
consulenza e semplicità

Rischio Cyber Security

Alavie
consulenza e semplifica

Rischio Cyber Security – Fattore Umano

L'anello debole della Cyber Security è il **fattore umano.**



Alavie

1.1 Elemento Soggettivo Esterno

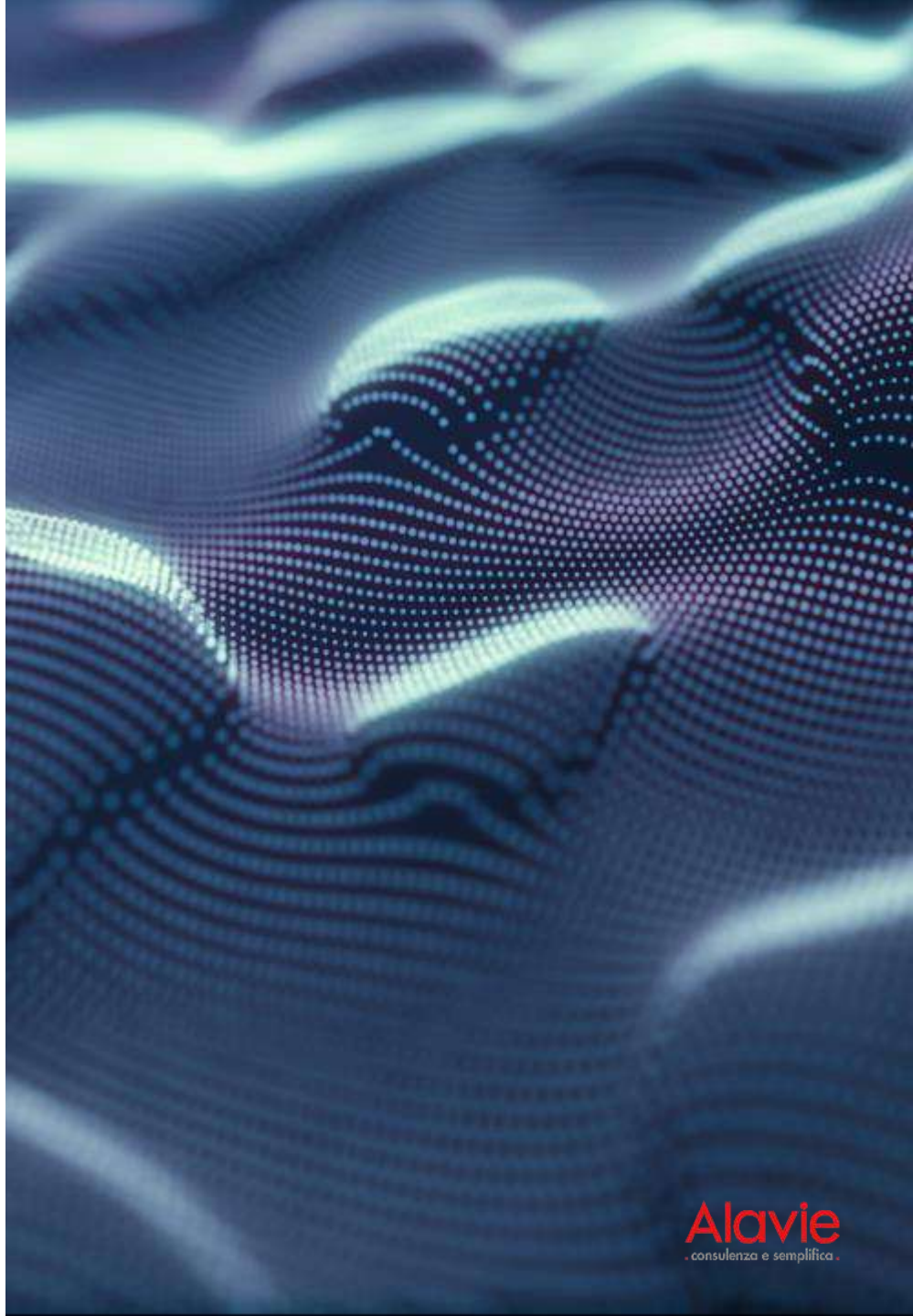
- **Attaccanti**: Esperti e profondi conoscitori dei sistemi informatici.
- **Organizzazioni**: esistono organizzazioni (equiparabili ad aziende) con una struttura gerarchica ben definita ed un affidamento di mansion specifiche, a seconda degli attacchi.
- **Modalità Operativa**: sfruttamento delle vulnerabilità.

1.2 Elemento Soggettivo Interno

- Rappresenta la **vulnerabilità maggiormente a rischio attacco** poiché lo stesso tende a sottovalutare le ripercussioni negative che, una insufficiente conoscenza in materia di *Cyber Security*, possono generare all'interno della realtà in cui opera.

Contenuti del modulo Cyber Security

1. Definizione di Cyber Security
2. Quadro Normativo Europeo e Nazionale
3. Rischio Cyber Security
4. **Attacco Cyber Security**
5. Tecniche di Attacco
6. Rapporto CLUSIT 2024
7. Misure di Sicurezza
8. Formazione Cyber Security



Attacco Cyber Security

ATTACCO INFORMATICO: tentativo di ottenere l' accesso non autorizzato a servizi, risorse o informazioni di sistema e/o di comprometterne l'integrità, ed in generale, consiste nell'atto intenzionale di tentare di eludere uno o più servizi di sicurezza o controlli di un sistema informativo digitale per alterare la Riservatezza, Integrità e Disponibilità (RID) dei dati - definizione del National Initiative For Cybersecurity Careers And Studies (NICCS) iniziativa nell'ambito del Cybersecurity and Infrastructure Security Agency (CISA).

Alavie

Principali informazioni bersaglio hacker

❑ **Codici fiscali e/o numeri di partita IVA dei clienti**

I criminali informatici possono utilizzare queste informazioni per mettere in atto tutta una serie di frodi e furti d'identità, come la registrazione di carte di credito con identità rubate e la messa a rischio di conti bancari e fascicoli sanitari tramite l'ingegneria sociale. Una volta che hanno accesso a determinate informazioni personali, sono già capaci di rovinare la vita della vittima.

Principali informazioni bersaglio hacker

- **Indirizzo, numero di telefono e data di nascita**

Tutti campi standard di un modulo 1040, si tratta delle altre informazioni che gli hacker cercano per creare conti bancari fittizi e appropriarsi di quelli esistenti.

Principali informazioni bersaglio hacker

- **Nome del coniuge, dei figli, luogo di lavoro e reddito annuale**

Per il furto dell'identità sono tutte informazioni utili che possono essere utilizzate per oltrepassare barriere di sicurezza come le domande di controllo. Insieme alle altre informazioni private menzionate in precedenza, gli hacker possono riuscire a ingannare il servizio clienti di un'azienda e ottenere accesso ai conti finanziari.

Principali informazioni bersaglio hacker

- **Fascicolo sanitario**

I moduli 1099-HC e le ricette mediche forniscono una serie di informazioni che gli hacker possono utilizzare per attuare frodi assicurative o mediche. In realtà, i fascicoli sanitari fanno incassare tanti soldi nello scambio di informazioni rubate.

Principali informazioni bersaglio hacker

- **Informazioni sul datore di lavoro**

I criminali che riescono ad accedere ai numeri di identificazione del datore di lavoro, alle informazioni dell'ufficio paghe e ai nomi dei contatti nel reparto amministrativo di un'organizzazione possono presentare note spese fraudolenti, fatture e richieste d'indennizzo assicurativo.

Principali informazioni bersaglio hacker

- **Registri finanziari**

Solitamente nei documenti fiscali e finanziari di fine anno che i clienti consegnano ai loro commercialisti sono contenuti i numeri di conto corrente bancario. È consuetudine diffusa che i contribuenti condividano anche le ricevute dei pagamenti con carta di credito riportanti le informazioni relative. Tali informazioni possono essere utilizzate per mettere in atto truffe con assegni e carte di credito o per accedere ai conti tramite la cosiddetta "ingegneria sociale".

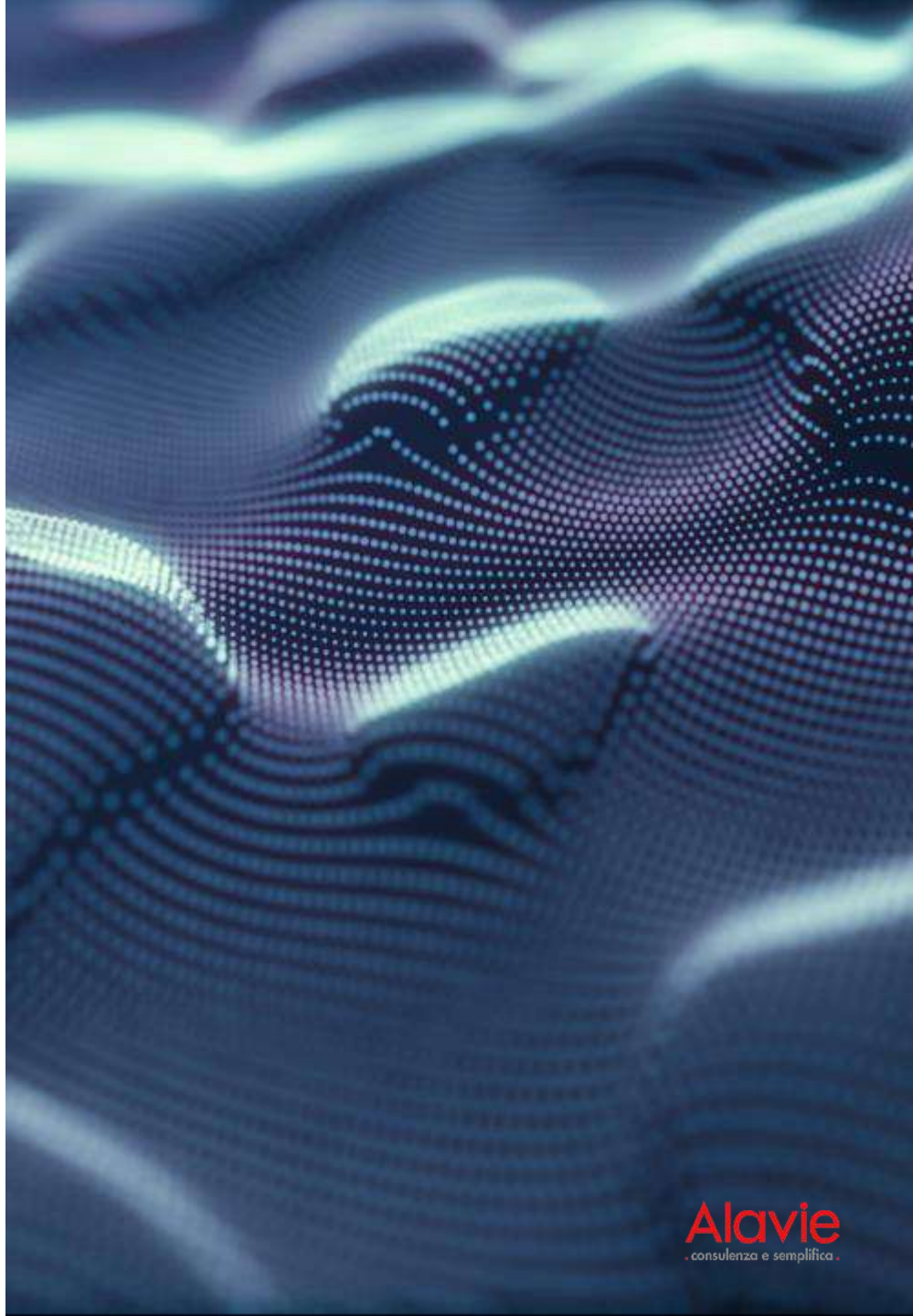
Principali informazioni bersaglio hacker

❑ **Indirizzi e-mail**

Armati di numero di conto corrente e di indirizzo e-mail, gli hacker possono riuscire a sottrarre i conti bancari e di intermediazione online tramite una semplice procedura di "password dimenticata?". Anche gli indirizzi e-mail possono essere raggirati, consentendo ai criminali di inviare messaggi verosimili ad altre persone che sembrano provenire da un mittente legittimo.

Contenuti del modulo Cyber Security

1. Definizione di Cyber Security
2. Quadro Normativo Europeo e Nazionale
3. Rischio Cyber Security
4. Attacco Cyber Security
5. **Tecniche di Attacco**
6. Rapporto CLUSIT 2024
7. Misure di Sicurezza
8. Formazione Cyber Security



Tecniche di attacco (1)

- **PHISHING/ E – MAIL SPOOFING** – Richiesta invio mail, messaggi per mezzo dei quali gli hackers si impossessano dei dati.
- **MAN IN THE MIDDLE (MITM o MIM)** – Letteralmente UOMO NEL MEZZO, si verifica l'attacco grazie all'intromissione dell'attaccante in una comunicazione tra due soggetti senza che questi se ne accorgano.

Tecniche di attacco (2)

- **ATTACCHI ALLA SUPPLY CHAIN** (catena di approvvigionamento) – Minacce avanzate e persistenti che possono compromettere il meccanismo di aggiornamento dei pacchetti software, permettendo ai criminali di inserirsi all'interno della distribuzione legittima del software stesso.
- **CROSS-SITE SCRIPTING (XSS)** – Vulnerabilità dei siti web che permette all'attaccante di agire da remoto sui dispositivi tramite l'inserimento di script dannosi all'interno del codice della pagina web.

Tecniche di attacco (3)

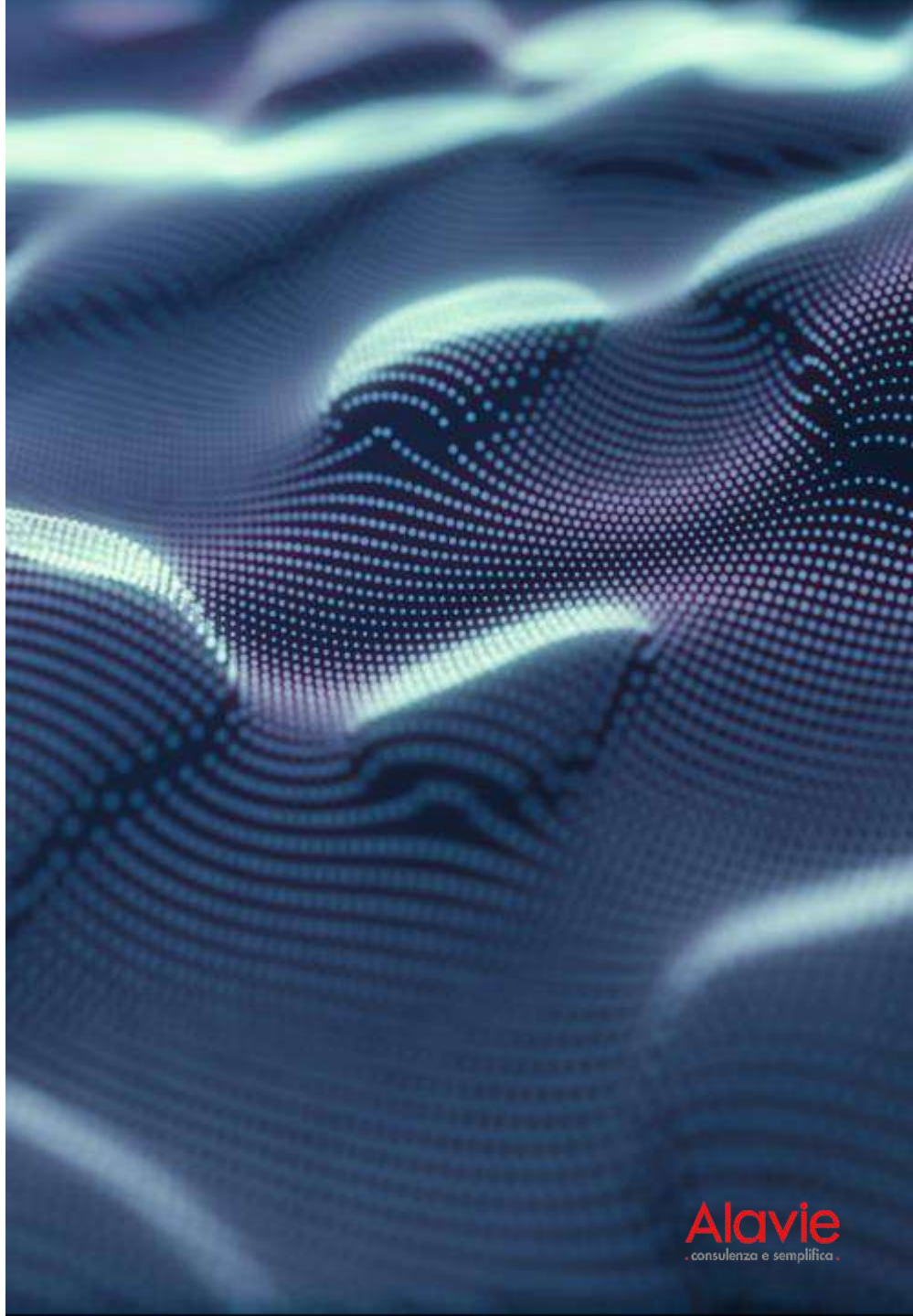
- **DENIAL OF SERVICE (DoS) e DISTRIBUTED DENIAL OF SERVICE (DDoS)** – Vulnerabilità più compromettenti per gli utenti. Si tratta di azioni malevole caratterizzate dall'ingolfamento del sistema attaccato (o del sito web) tramite BOTNET (insieme di computer infettati da malware che consentiranno il controllo al cybercriminale.

Tecniche di attacco (4)

- **MALWARE** – Software malevoli:
  - **VIRUS** – Si propaga «agganciandosi» ad altri programmi e provoca la distruzione dati;
  - **WORM** – Si diffonde autonomamente nel cyberspazio (es: mail, reti informatiche, etc.);
  - **TROJAN HORSE** – Falsa identità che induce l'attaccato a a installare programma malevole;
  - **RANSOMWARE** – Criptazione di tutti i dati e conseguente blocco totale della macchina.

Contenuti del modulo Cyber Security

1. Definizione di Cyber Security
2. Quadro Normativo Europeo e Nazionale
3. Rischio Cyber Security
4. Attacco Cyber Security
5. Tecniche di Attacco
6. **Rapporto CLUSIT 2024**
7. Misure di Sicurezza
8. Formazione Cyber Security



Rapporto CLUSIT 2024

- Nel periodo in esame, tra gennaio 2019 e dicembre 2023 si sono verificati un totale di **10.858** cyber attacchi, suddivisi come mostrato in Fig. 1.

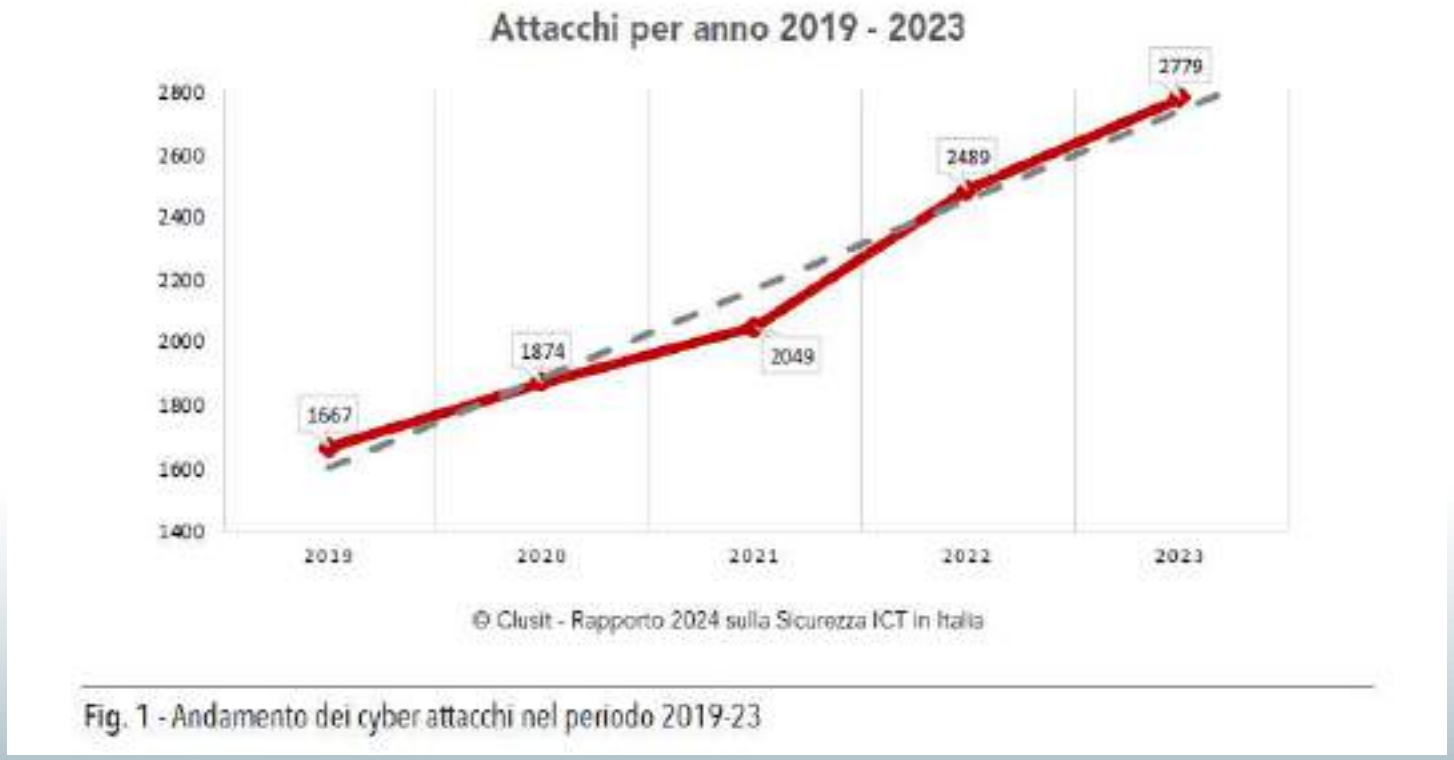


Fig. 1 - Andamento dei cyber attacchi nel periodo 2019-23

- Il **56%** degli incidenti censiti dal 2011 sono avvenuti negli ultimi 5 anni

Alavie

- A livello di distribuzione mensile, la prima metà dell'anno vede registrare una attività molto più intensa, con un picco massimo ad aprile 2023 con 270 attacchi, raggiungendo un record negativo mai raggiunto, come mostrato nella Fig. 2

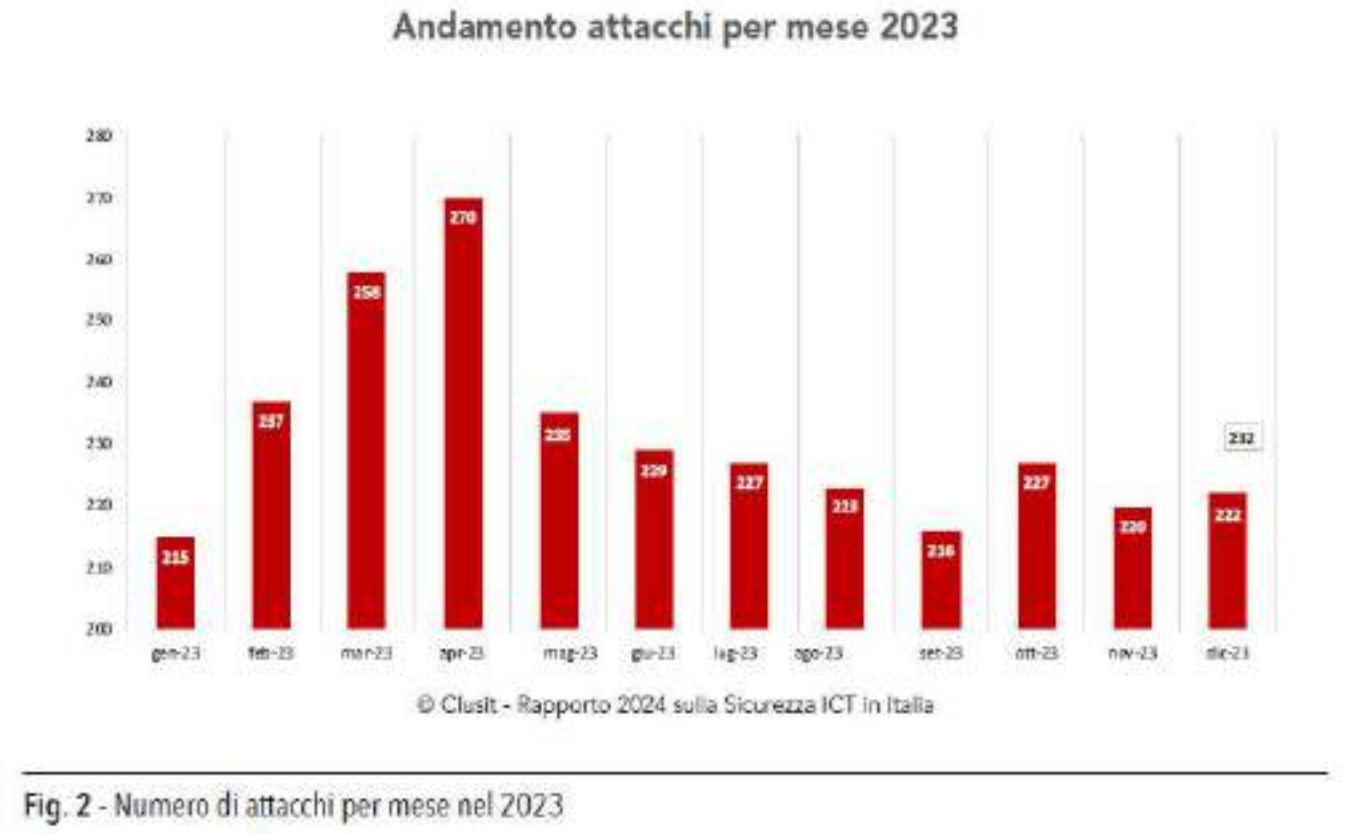


Fig. 2 - Numero di attacchi per mese nel 2023

Anche la media mensile dei cyber attacchi (Fig. 3) è aumentata, arrivando a 232, con una tendenza di crescita costante, considerando che nel 2019 si attestava a poco più della metà.

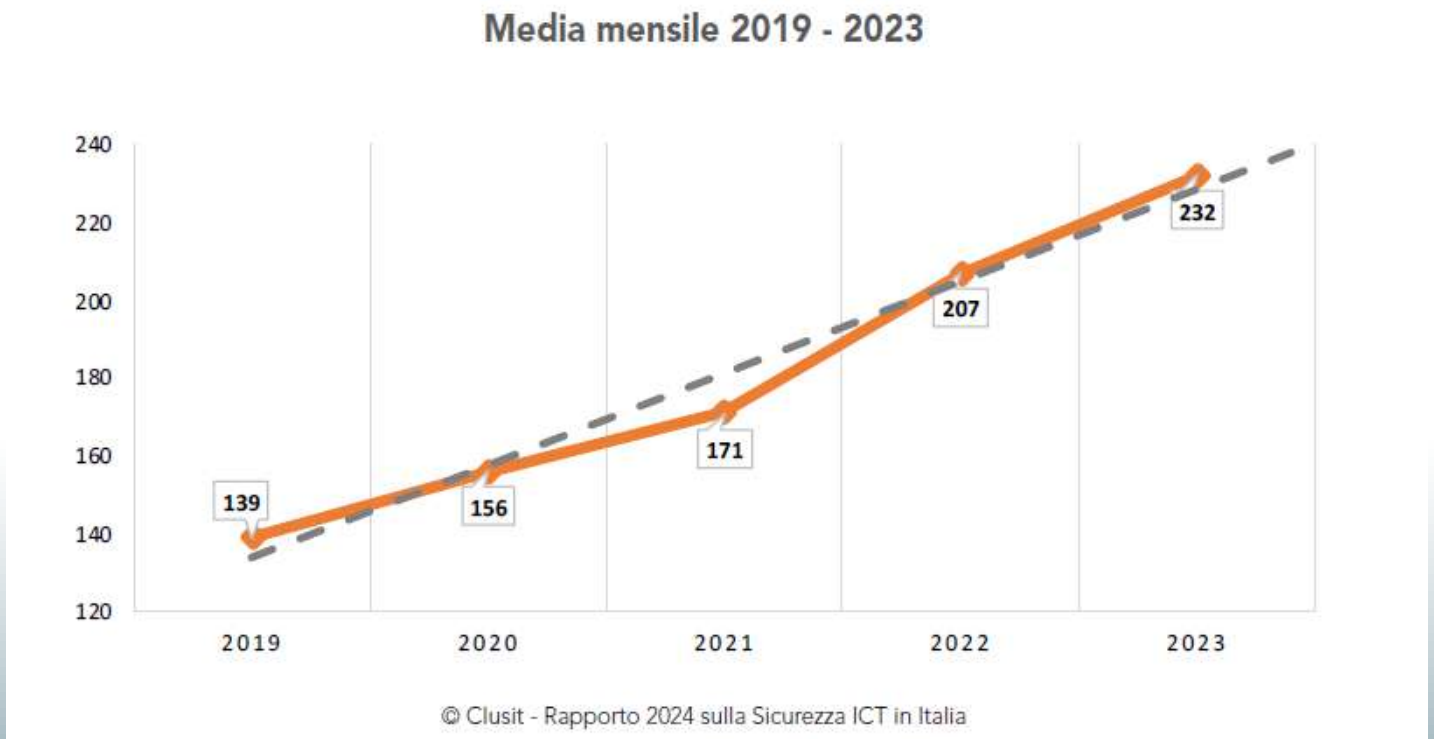


Fig. 3 - Andamento delle medie mensili nel periodo 2019-23

Il confronto della distribuzione degli attaccanti nel periodo dal 2019 al 2023 (Fig. 4) evidenzia in modo chiaro che **il *Cybercrime* continua a rimanere la motivazione principale degli incidenti**, con un andamento regolarmente in crescita negli anni (+13,4% nel 2023 rispetto all'anno precedente).

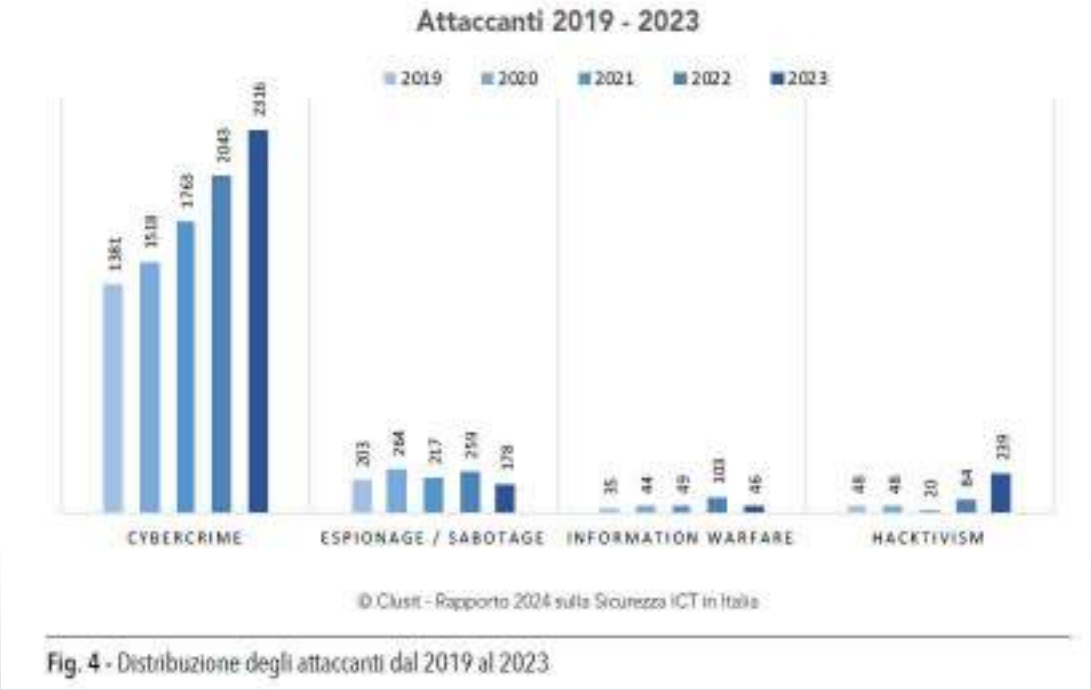


Fig. 4 - Distribuzione degli attaccanti dal 2019 al 2023

Al contrario, i fenomeni di *Espionage* e *Information Warfare* mostrano una diminuzione significativa. Aumentano invece gli attacchi dovuti ad **attività di Hacktivism**, che quasi triplicano, passando dagli 84 del 2022 ai 239 del 2023.

Alavie
consulenza e semplicità

Crescono in modo consistente i **settori Financial/Insurance ed Healthcare**, quest'ultimo il settore specifico più colpito dopo la categoria Multiple target. Restano stabili gli incidenti che colpiscono il settore ICT e **aumentano in modo consistente quelli verso Manifacturing, Professional / Scientific / Technical, Transportation / Storage, Wholesale / Retail**

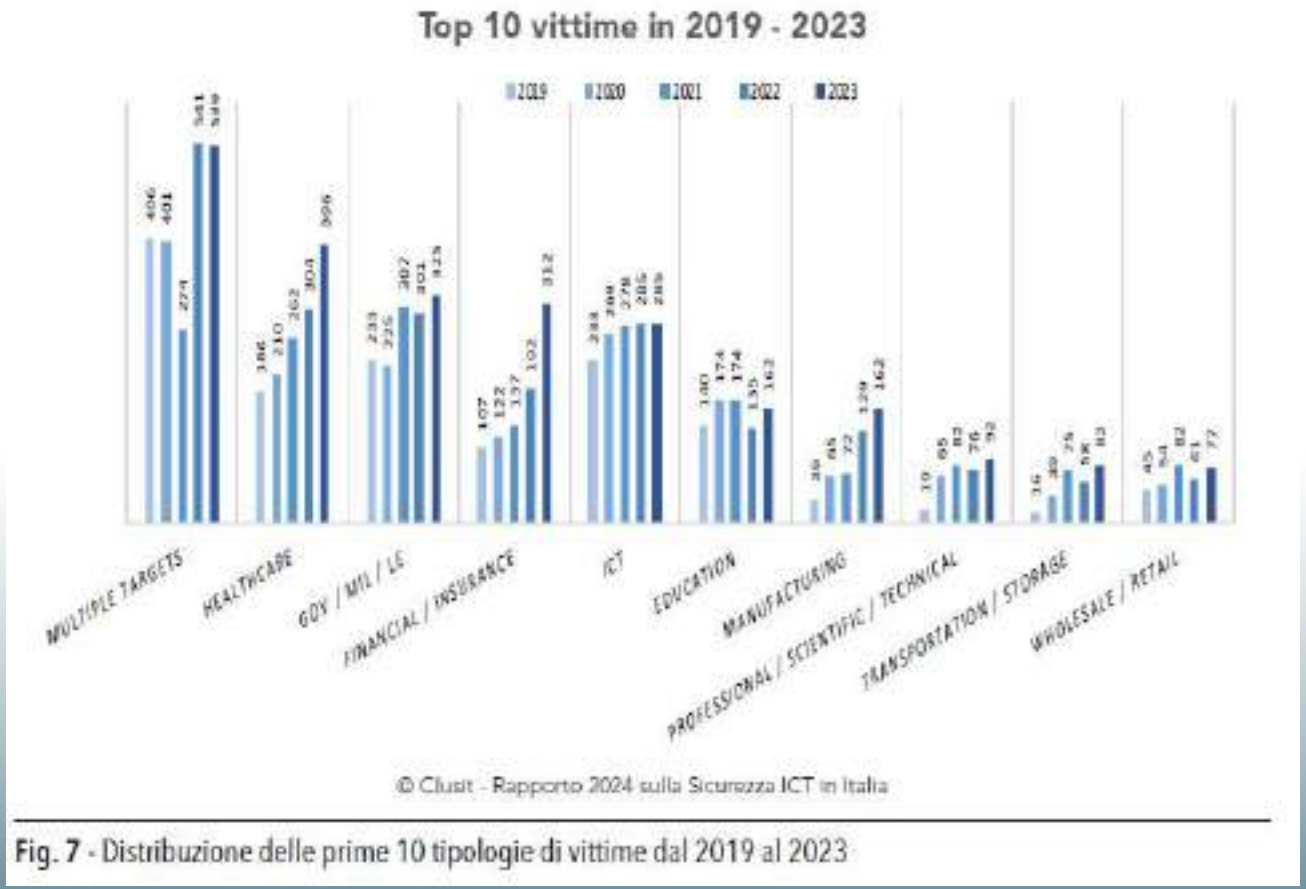


Fig. 7 - Distribuzione delle prime 10 tipologie di vittime dal 2019 al 2023

La situazione nazionale diventa preoccupante se confrontata,
in termini di percentuali di crescita, rispetto al dato globale: all'aumento del **65%** segnato dagli attacchi italiani corrisponde infatti un molto più contenuto +12% complessivo.

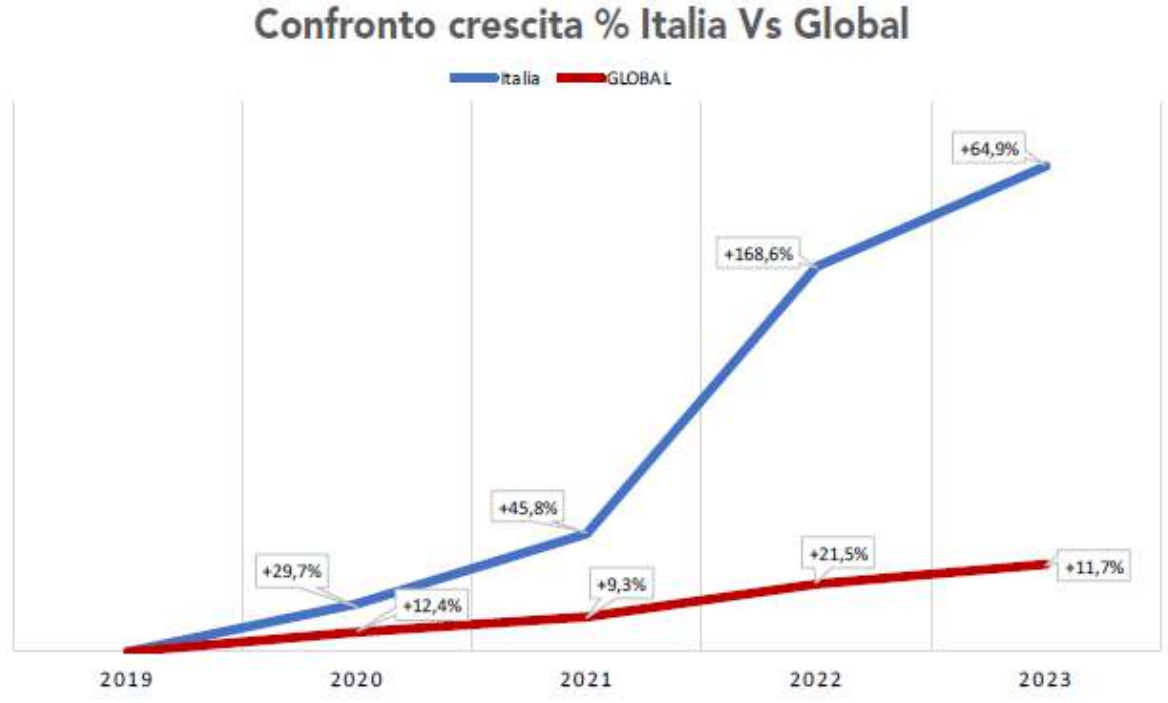


Fig. 28 - Crescita percentuale degli attacchi Italia vs. global - 2019-2023

Alavie
consulenza e semplifica

Gli incidenti ***Cybercrime,*** nell'ultimo anno hanno subito un **aumento del 13%,** passando da 175 a 197 attacchi rilevati (Fig. 31).
Il trend più significativo è costituito dall'aumento degli attacchi di tipologia ***Hacktivism***, che passano dal 7% del campione nel 2022 (13 eventi) al 36% del 2023 (112 eventi), con un **aumento del 761%**

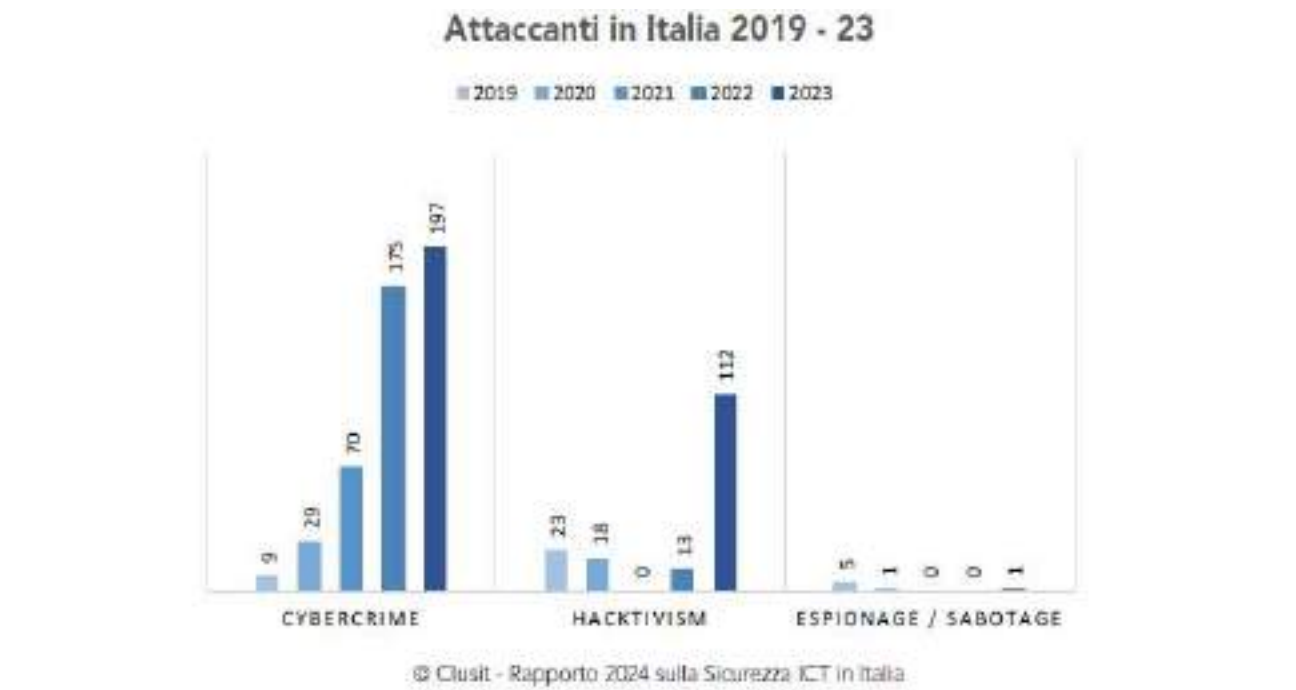
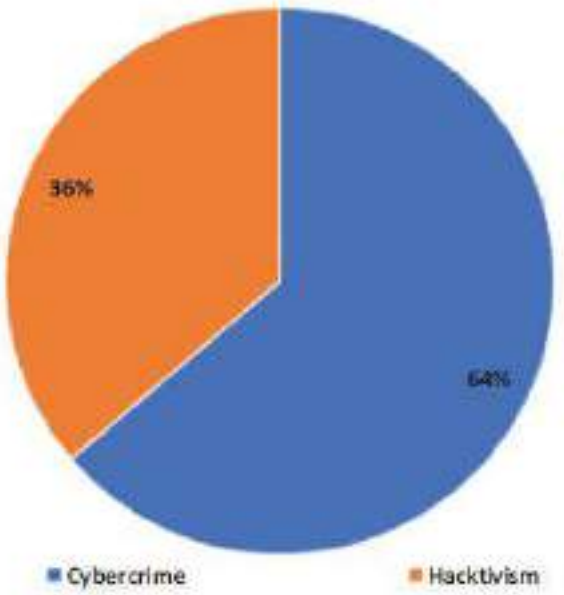


Fig. 31 - Attaccanti in Italia nel periodo 2019-2023

In Italia, la maggioranza degli attacchi noti si riferisce alla categoria ***Cybercrime***, che rappresenta il **64%.**
Seguono con il **36%** gli incidenti classificati come ***Hacktivism***, dovuti al conflitto in Ucraina, nei quali gruppi di attivisti agiscono mediante campagne dimostrative rivolte tanto al nostro Paese che alle altre nazioni del blocco filo-ucraino.



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

Fig. 30 - Attaccanti in Italia nel 2023

Tecniche di attacco in Italia 2022

Dalla Fig. 35 si evince che la tecnica dominante è costituita dagli attacchi DDoS, che
passano dal 4% del 2022 a ben il 36% di quest'anno, dato trainato in modo rilevante dall'aumento di incidenti causati da campagne di Hacktivism.

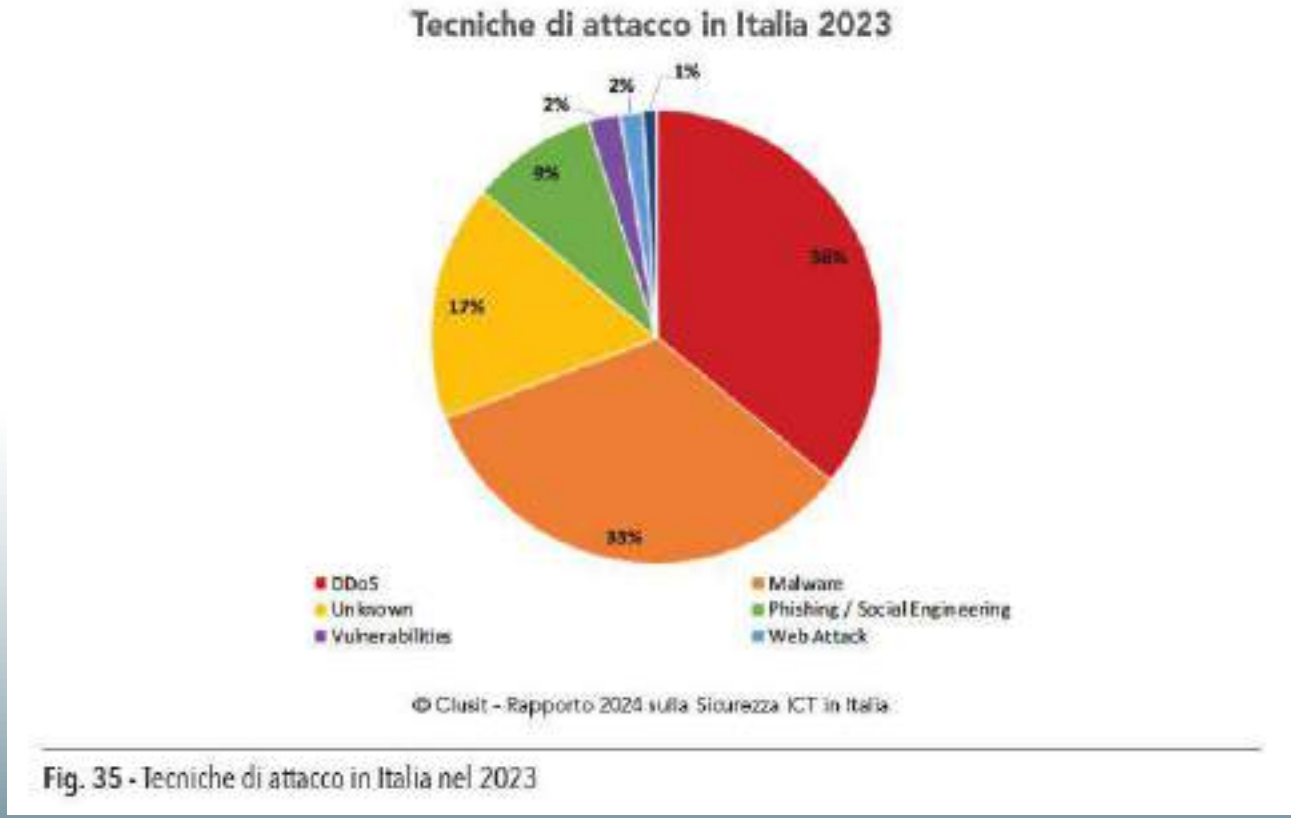


Fig. 35 - Tecniche di attacco in Italia nel 2023

Quanto costa un attacco cyber?

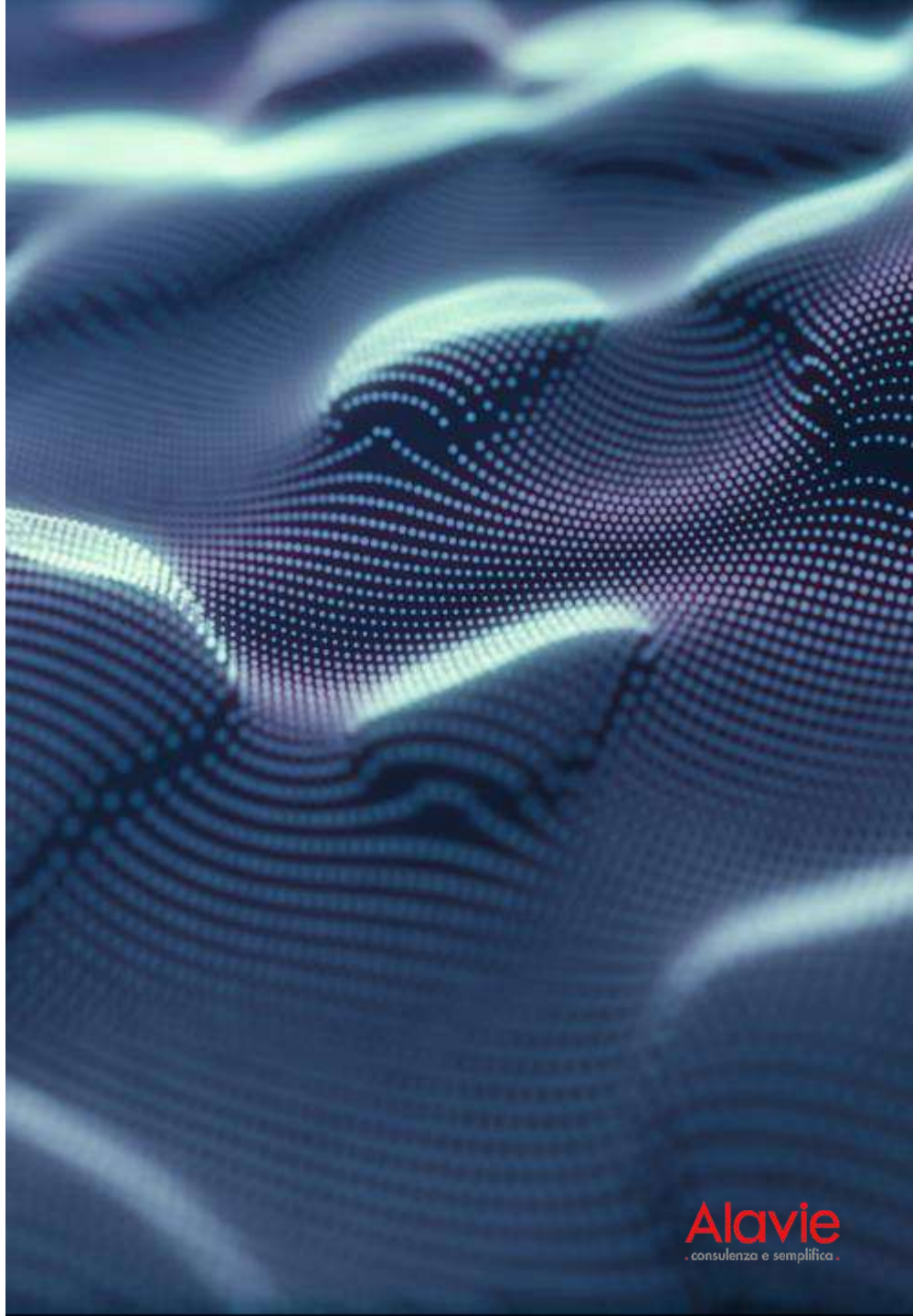
- Secondo il Report Cost of a Data Breach 2023, **il costo medio globale di una violazione dei dati ha raggiunto il valore di 4,45 milioni di dollari nel 2023** (massimo storico per il report) in aumento del 15% negli ultimi tre anni.

- Il **51%** delle organizzazioni prevede di aumentare gli **investimenti in sicurezza** a seguito di una violazione, compresa la pianificazione e i test di risposta agli incidenti (IR), la formazione dei dipendenti e gli strumenti di rilevamento e risposta alle minacce.

Alavie

Contenuti del modulo Cyber Security

1. Definizione di Cyber Security
2. Quadro Normativo Europeo e Nazionale
3. Rischio Cyber Security
4. Attacco Cyber Security
5. Tecniche di Attacco
6. Rapporto CLUSIT 2024
7. **Misure di Sicurezza**
8. Formazione Cyber Security



Misure di Sicurezza applicate ai dati

- CRITTOGRAFIA
- ANONIMIZZAZIONE
- PARTIZIONAMENTO
- CONTROLLO ACCESSI LOGICI
- TRACCIABILITA’
- MINIMIZZAZIONE DATI
- ARCHIVIAZIONE
- SICUREZZA DOCUMENTI CARTACEI

Misure di Sicurezza applicate ai Sistemi

- Vulnerabilita’
- Lotta contro il malware
- Gestione postazioni
- Sicurezza siti web
- Back up
- Manutenzione
- Controllo accessi fisici
- Tracciabilita’
- Sicurezza HW

Misure di Sicurezza ORGANIZZATIVE

- Politica tutela privacy
- Procedure gestione delle politiche di tutela privacy
- Politica gestione rischi
- Procedure gestione incident di sicurezza e violazione dei dati
- Procedure privacy e cybersecurity nei progetti
- Piano e procedure gestione dipendenti
- Procedura gestione terzi che accedono ai dati

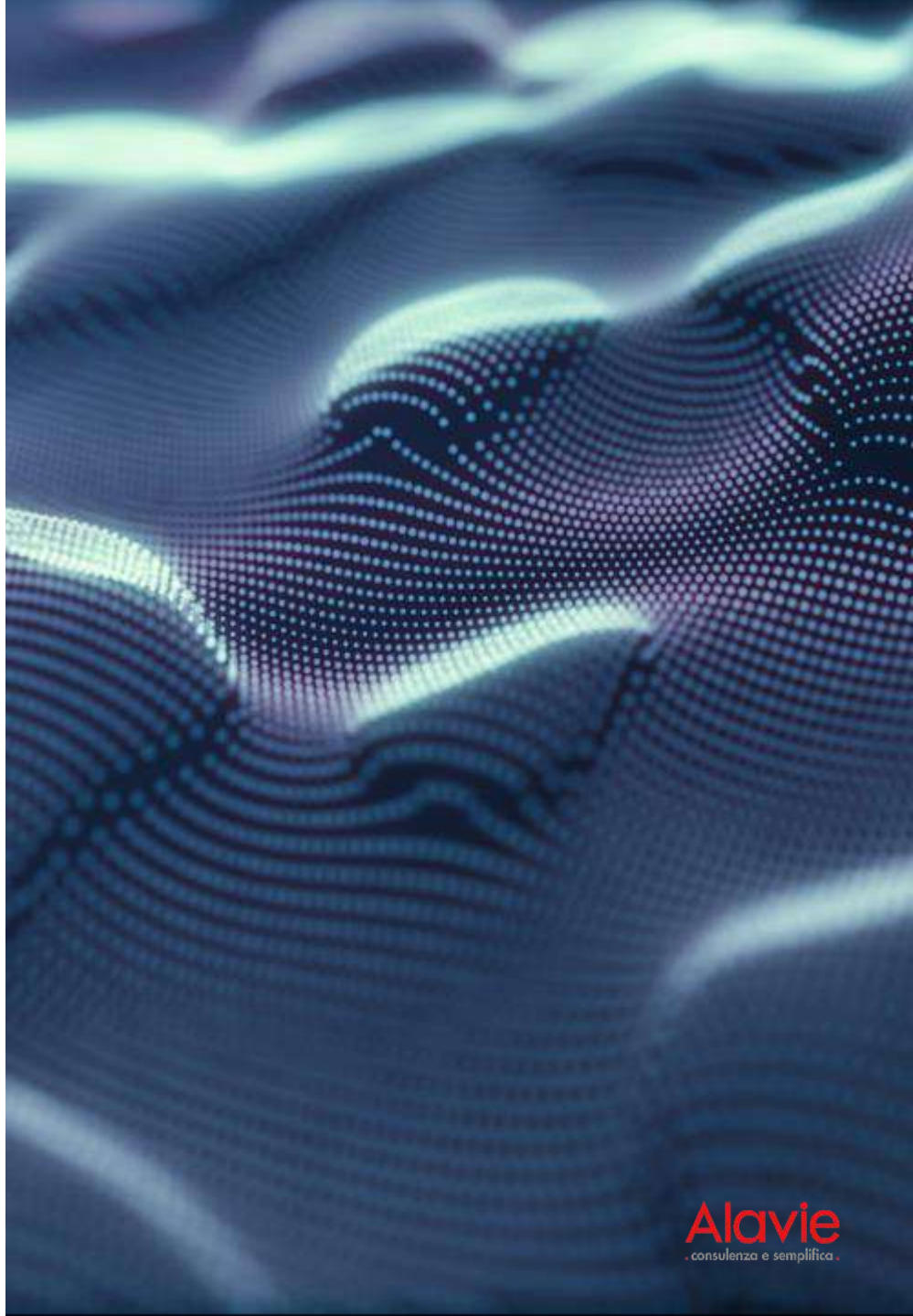
Password sicure: le linee guida del garante e ACN

Provvedimento 7 Dicembre 2023: « LINEE GUIDA FUNZIONI CRITTOGRAFICHE-CONSERVAZIONI DELLE PASSWORD»

- **Implementazione delle funzioni crittografiche**, le tecniche più sicure per la conservazione delle password;
- **Complessità** computazionale adeguata;
- **Cancellazione** tempestiva delle password una volta terminata la finalità per cui sono state implementate;
- **COMPETENZE E CONSAPEVOLEZZA**: l'attività formativa di tutti gli incaricati deve essere continuativa, metodologica e strategicamente strutturata ad ogni livello aziendale.

Contenuti del modulo Cyber Security

1. Definizione di Cyber Security
2. Quadro Normativo Europeo e Nazionale
3. Rischio Cyber Security
4. Attacco Cyber Security
5. Tecniche di Attacco
6. Rapporto CLUSIT 2024
7. Misure di Sicurezza
8. **Formazione Cyber Security**



Formazione Cyber Security

01

CREAZIONE DI UNA **CULTURA DELLA SICUREZZA INFORMATICA** ALL'INTERNO DELLA PROPRIA REALTA'

02

DEFINIZIONE DI **POLITICHE, STRATEGIE E PROCEDURE** PER GARANTIRE SICUREZZA DEI DATI, DELLE RETI E DEI SISTEMI

03

APPLICAZIONE DI **CONTROLLI PERIODICI** PER LA MITIGAZIONE DEI RISCHI CYBER

Alavie
consulenza e semplifica

Alavie

. consulenza e semplifica .

www.alavie.it

contattaci@alavie.it