

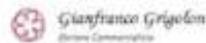


VESCOGIARETTA GROUP

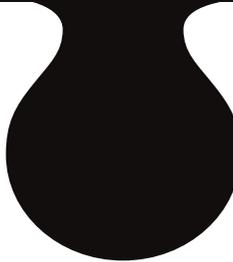
IL GARANTE INCONTRA LE IMPRESE: PRIVACY E REGOLAMENTO UE N679/2016

Villa "Le Colombare", 15 Marzo 2018

IN COLLABORAZIONE CON



IL GARANTE INCONTRA LE IMPRESE: PRIVACY E REGOLAMENTO UE N. 679/2016



Dott.ssa Cinzia Giaretta
VESCOGIARETTA GROUP

IL REGOLAMENTO EUROPEO E L'IMPATTO NELLA LEGISLAZIONE ITALIANA: CRITICITA', ADEMPIMENTI E PROSPETTIVE

Avv. Federica Resta

Garante per la Protezione dei Dati Personali, Roma

IL NUOVO REGOLAMENTO E IL SUO IMPATTO
SU AZIENDE E PROFESSIONISTI.
LA FIGURA DEL DPO

Avv. Rosanna Filippin
VESCOGIARETTA GROUP

REGOLAMENTO EUROPEO IN MATERIA DEI DATI PERSONALI (679/2016)

Relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati

DIRETTIVA EUROPEA 680 /2016

Relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento, perseguimento di reati ed esecuzione di sanzioni penali

ENTRA IN VIGORE IL 25 MAGGIO 2018
NON SOSTITUISCE IL CODICE PRIVACY (196/2003)
che resta in vigore per le parti non in contrasto

SCOPO : RAFFORZARE E RENDERE OMOGENEA
LA PROTEZIONE DATI PERSONALI DEI CITTADINI UE
UNIFICARE LE REGOLE PRIVACY DEGLI STATI UE

DEFINIZIONE di DATO PERSONALE

QUALSIASI INFORMAZIONE RIGUARDANTE
UNA PERSONA FISICA IDENTIFICATA O
IDENTIFICABILE.

Identificabile è la persona fisica che può essere identificata, direttamente o indirettamente, con riferimento ad un nome, numero di identificazione, dati di ubicazione, identificativo online o ad uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

A CHI SI APPLICA IL REGOLAMENTO EUROPEO PROTEZIONE DATI PERSONALI?

A tutte le organizzazioni (compresa p.a.) che trattano dati personali di soggetti che si trovano nell'unione senza alcun limite alla dimensione dell'organizzazione



I RUOLI COINVOLTI

DATA CONTROLLER O TITOLARE DEL TRATTAMENTO

Soggetto (persona fisica o giuridica, P.A. e qualsiasi altro ente, associazione ed organismo) che determina le finalità e i mezzi del trattamento dei dati personali

DATA PROCESSOR O RESPONSABILE DEL TRATTAMENTO

Soggetto esterno che esegue, in base a contratto/convenzione od altro atto giuridico, il trattamento dei dati personali per conto del titolare del trattamento e ne risponde in solido in caso di inadempienze

DATA PROTECTION OFFICER (DPO) O RESPONSABILE PROTEZIONE DEI DATI

Soggetto con il compito di facilitare l'osservanza del regolamento attraverso strumenti di accountability e di interfaccia fra i soggetti coinvolti

DATA PROTECTION AUTHORITY O GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

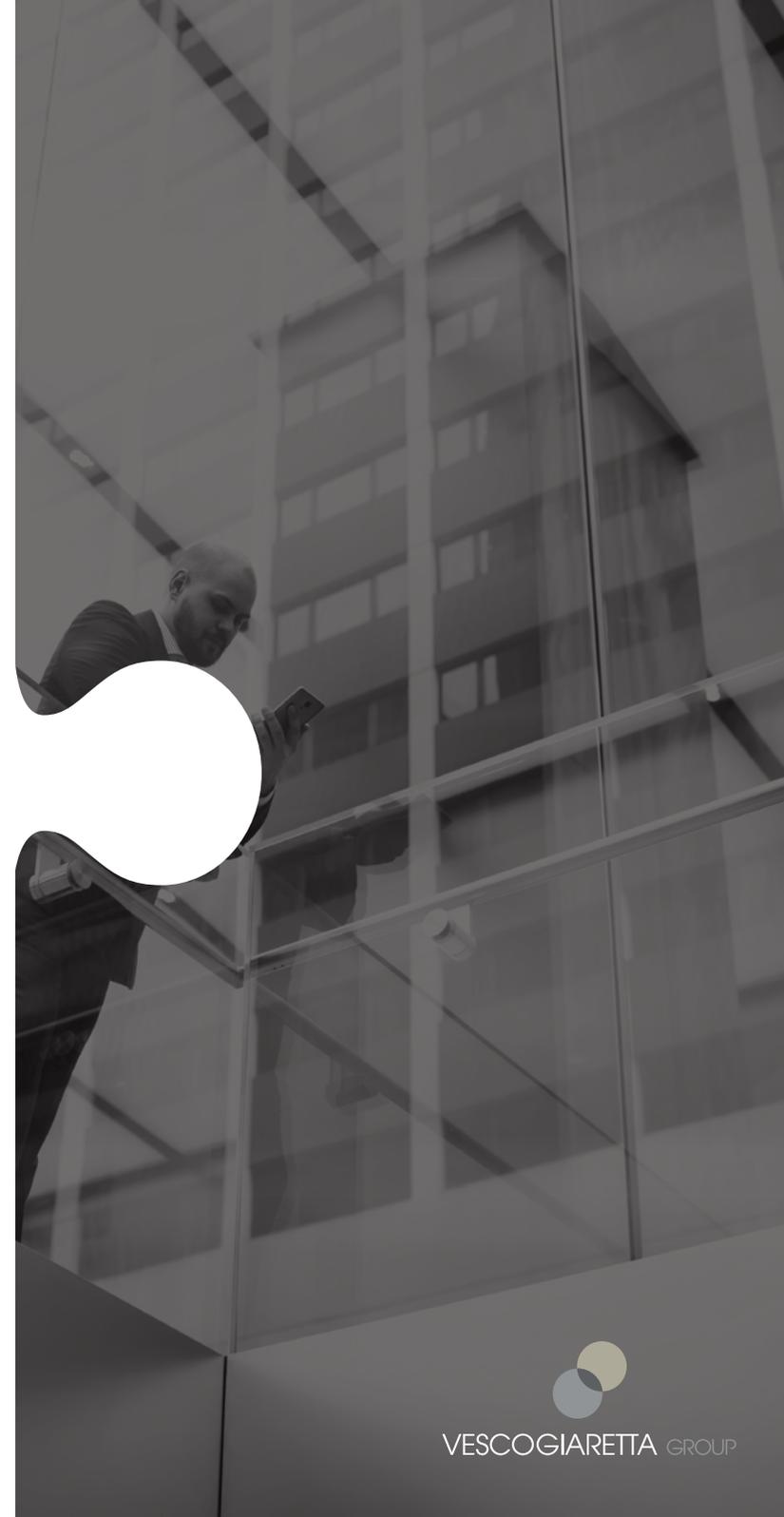
DATA SUBJECT O SOGGETTO INTERESSATO



CITTADINI AL CENTRO DEL SISTEMA

ASSICURARE UN LIVELLO ELEVATO ED UNIFORME
DI TUTELA DEI DATI MAGGIOR CONTROLLO AI
CITTADINI SULL'UTILIZZO DEI LORO DATI

- 1 Diritto ad essere informato in modo trasparente, leale e dinamico sui trattamenti effettuati sui suoi dati
- 2 Diritto di controllare i trattamenti effettuati sui suoi dati
- 3 Diritto ad essere informato sulle violazioni dei propri dati personali (data breach)
- 4 Diritto alla portabilità dei dati
- 5 Diritto all'oblio



PRINCIPIO BASE REGOLAMENTO
UE PRIVACY :

ACCOUNTABILITY O RESPONSABILIZZAZIONE DI TITOLARI E RESPONSABILI DEL TRATTAMENTO

Adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento e dunque la protezione dei dati personali

DATA PROTECTION BY DESIGN
AND BY DEFAULT

PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA

Configurare il trattamento prevedendo sin dall'inizio le garanzie per la tutela dei dati personali, tenendo conto del contesto ove il trattamento si colloca e i rischi per i diritti e le libertà degli interessati.

Quindi analisi preventiva ed impegno di applicazione della



OBBLIGHI SPECIFICI IN CAPO AI TITOLARI ED AI RESPONSABILI DEL TRATTAMENTO

TENUTA DEL REGISTRO DEI TRATTAMENTI

Registro in forma scritta (anche elettronica) delle operazioni di trattamento dati personali, indispensabile per ogni valutazione ed analisi di rischio. Da esibire su richiesta del Garante. Obbligatorio per organismi con 250 dipendenti ed oltre oppure se si effettuano trattamento dati

ADOZIONE DI IDONEE MISURE TECNICHE ED ORGANIZZATIVE PER GARANTIRE LA SICUREZZA DEI TRATTAMENTI

(Messa in sicurezza di persone, processi, tecnologia)

NOTIFICA DELLE VIOLAZIONI DI DATI PERSONALI

Entro 72 ore se derivano rischi per i diritti e libertà interessato

IN CASO DI VIOLAZIONI del REGOLAMENTO SONO PREVISTE SANZIONI

COMMISURATE ALLA NATURA,
GRAVITÀ E DURATA DELLA VIOLAZIONE.

- Fino a **10 milioni di euro** o, in caso d'impresa, fino al **2 % fatturato** per violazioni degli obblighi del Titolare del Trattamento o del DPO.
- Fino a **20 milioni di euro**, o in caso di impresa, **fino al 4% del fatturato**, per violazioni dei principi base del trattamento (consenso, diritti degli interessati, mancata ottemperanza all'ordine della autorità di vigilanza)

FONDAMENTI DI LICEITA' DEL TRATTAMENTO DEL DATO PERSONALE

CONSENSO preventivo ed inequivocabile anche se espresso con mezzi elettronici.

Se dati sensibili, il consenso deve essere esplicito.

Revocabile sempre.

ADEMPIMENTI OBBLIGHI CONTRATTUALI
INTERESSI VITALI DELL'INTERESSATO O DI UN TERZO
OBBLIGHI DI LEGGE
INTERESSE PUBBLICO O ESERCIZIO DI PUBBLICI POTERI



INFORMATIVA

PRIMA DI EFFETTUARE LA RACCOLTA DATI
INFORMATIVA **CONCISA, TRASPARENTE,
COMPENSIBILE E FACILMENTE ACCESSIBILE**

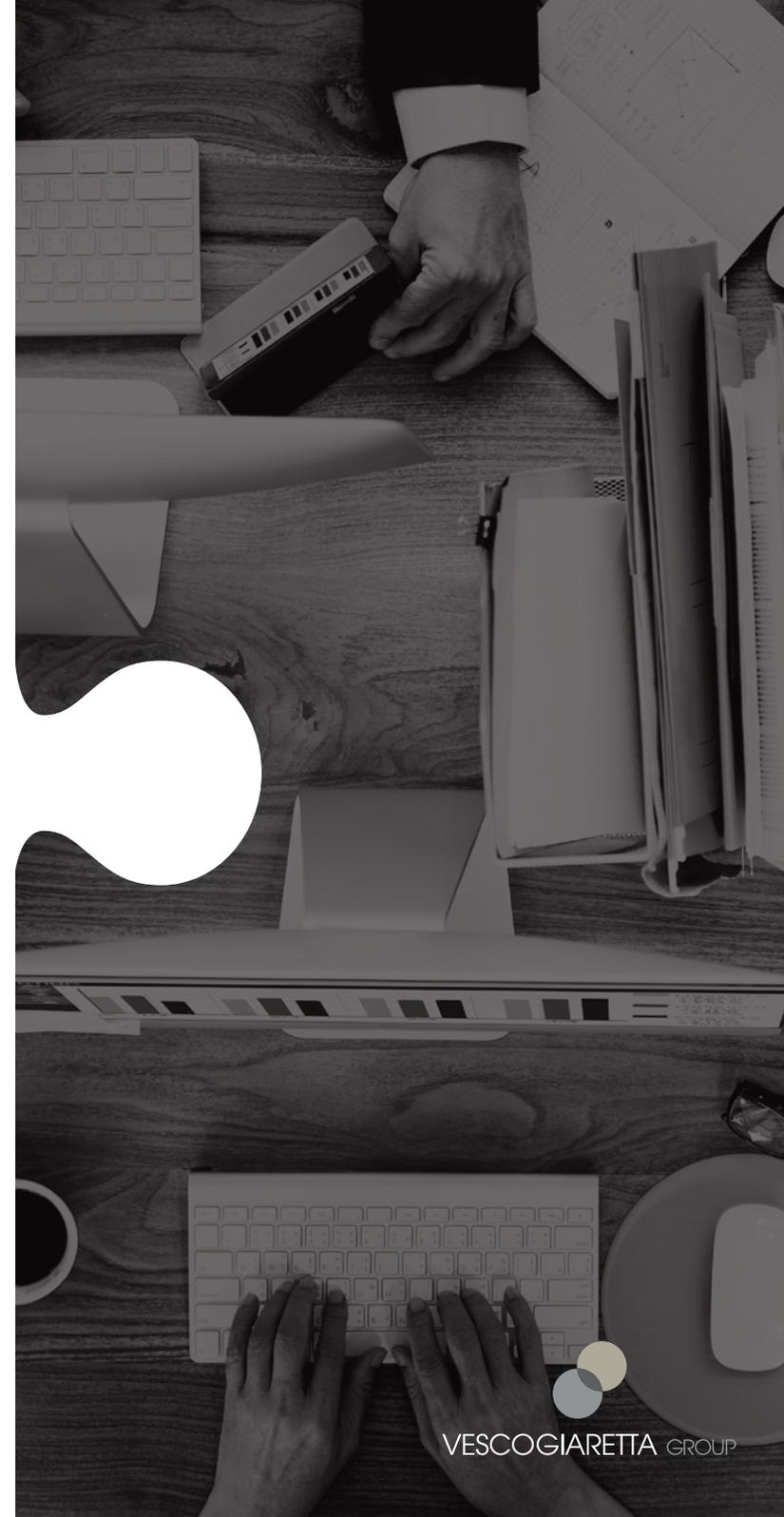
Sempre specificati:

- i dati del titolare del trattamento
- il dpo (se nominato)
- la base giuridica del trattamento

Se ci sarà trasferimento dati personali

In paese terzi

- periodo di conservazione dei dati
- modalita' di presentazione reclamo



COMPITI e FUNZIONI del RESPONSABILE DELLA PROTEZIONE DEI DATI (D.P.O.)

- SOGGETTO INTERNO / ESTERNO CHE AGISCE IN AUTONOMIA
- FACILITA e SORVEGLIA L'APPLICAZIONE DEL REGOLAMENTO
- FUNGE DA COLLEGAMENTO FRA IL TITOLARE / RESPONSABILE del TRATTAMENTO,
- COADIUVA IL TITOLARE / RESPONSABILE NELLA VALUTAZIONE D'IMPATTO E NELLA REDAZIONE DEL REGISTRO DEI TRATTAMENTI
- INFORMA E FORNISCE CONSULENZA AL TITOLARE / RESPONSABILE ED AL PERSONALE INTERNO SULL'APPLICAZIONE DEL GDPR
- AMPIO ACCESSO ALLE INFORMAZIONI ED ESSERE INTERPELLATO PER OGNI PROBLEMATICHE SUL TRATTAMENTO DATI



NOMINA OBBLIGATORIA DPO

SE TRATTAMENTO E' SVOLTO DA UN'AUTORITA' PUBBLICA O DA ORGANISMO PUBBLICO

SE ATTIVITA' PRINCIPALI CONSISTONO IN TRATTAMENTI CHE RICHIEDONO MONITORAGGIO REGOLARE E SISTEMATICO DI INTERESSATI SU LARGA SCALA

SE ATTIVITA' PRINCIPALI CONSISTONO NEL TRATTAMENTO SU LARGA SCALA DI PARTICOLARI TIPI DI DATI

(dati personali che rivelino origine razziale o etnica, opinioni politiche, convinzioni filosofiche o religiose, appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute, vita sessuale o orientamento sessuale)

O DATI PERSONALI RELATIVE A CONDANNE PENALI

QUALITA' DEL D.P.O

- Conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione dati.
- Familiarità con le operazioni di trattamento svolte.
- Familiarità con tecnologie informatiche e misure di sicurezza dei dati.
- Conoscenza del settore di attività e dell'organizzazione del titolare / responsabile.
- Capacità di promuovere la cultura della protezione dati all'interno dell'organizzazione.

+ INDIPENDENZA,
+ AUTOREVOLEZZA,
+ ASSENZA DI CONFLITTI DI INTERESSE
+ COMPETENZE MANAGERIALI



PER FINIRE

ALCUNE DOMANDE CHIAVE

- 1 QUALI DATI PERSONALI SONO TRATTATI ?
- 2 DOVE SONO E QUAL È IL FLUSSO SIA DALL'INTERNO DELL'ORGANIZZAZIONE CHE ALL'ESTERNO ?
- 3 COME VENGONO ELABORATI, PROTETTI, MEMORIZZATI, CANCELLATI ?
- 4 COME LA PRIVACY È STATA RAGGIUNTA AI DIVERSI LIVELLI ? VANNO RIVISTE LE DISPOSIZIONI PER LA GESTIONE DEL RISCHIO ?
- 5 ESISTONO MISURE ADEGUATE PER RIDURRE I RISCHI, GLI ATTACCHI E LA VIOLAZIONI DI DATI ?
- 6 ESISTONO PROCEDURE PER IL RILEVAMENTO E LA RISPOSTA AGLI ATTACCHI ?



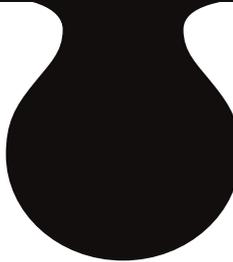
PRIVACY E CYBER SECURITY: LA STRATEGIA PER ESSERE IN REGOLA

3 Diego Zanella
Sistemi Contabili S.p.a

SOLUZIONI ASSICURATIVE SUL CYBER RISK

Evelin Gottardi
Mec.Vis. S.r.l.

IL GARANTE INCONTRA LE IMPRESE: PRIVACY E REGOLAMENTO UE N. 679/2016



Dott. Antonio Vesco
VESCOGIARETTA GROUP