MRP | AVVOCATO MARIA ROBERTA PERUGINI

GDPR-La privacy nella pratica quotidiana

Tutte le domande a cui un DPO deve sapere rispondere

Appendici

Appendice A – Dati Personali

«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un

- identificativo come il nome
- un numero di identificazione
- dati relativi all'ubicazione
- un identificativo online

o a uno o più elementi caratteristici della sua identità

- fisica
- fisiologica
- genetica
- psichica
- economica
- culturale
- sociale;

GDPR – categorie particolari di dati (art. 9)

Dati personali che rivelino:

- origine razziale o etnica
- opinioni politiche
- convinzioni religiose o filosofiche
- l'appartenenza sindacale

Dati personali relativi:

- alla salute
- alla vita sessuale
- all'orientamento sessuale
- dati genetici
- dati biometrici intesi a identificare in modo univoco una persona fisica

GDPR – Dati genetici (art. 4-13 *C34*)

«dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

È opportuno che per dati genetici si intendano i dati personali relativi alle caratteristiche genetiche, ereditarie o acquisite, di una persona fisica, che risultino dall'analisi di un campione biologico della persona fisica in questione, in particolare dall'analisi dei cromosomi, dell'acido desossiribonucleico (DNA) o dell'acido ribonucleico (RNA), ovvero dall'analisi di un altro elemento che consenta di ottenere informazioni equivalenti.

GDPR – Dati biometrici (art. 4-14 *C51*)

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

… Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica…

GDPR – Dati relativi alla salute (art. 4-15 *C35*)

«dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

Nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio; un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro.

Garante per la protezione dei dati personali

Guida alla *Notificazione del trattamento dei dati personali (artt. 7, 16 e 28 legge 31 dicembre 1996, n. 675)*

Tratto da **Allegato c) - elenco delle categorie di dati oggetto del trattamento**

CATEGORIE DI DATI OGGETTO DI TRATTAMENTO
Codice fiscale ed altri numeri di identificazione personale *(carte sanitarie)*
Nominativo, indirizzo o altri elementi di identificazione personale *(nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro, numero di telefono, di telefax o di posta elettronica, posizione rispetto agli obblighi militari, numero carta di identità, passaporto, patente di guida, numero di posizione previdenziale o assistenziale, targa automobilistica, dati fisici (altezza, peso, ecc)*
Dati relativi alla famiglia e a situazioni personali *(stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare)*
Lavoro *(occupazione attuale e precedente, informazioni sul reclutamento, sul tirocinio o sulla formazione professionale, informazioni sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione, curriculum vitae o lavorativo, competenze professionali, retribuzioni, assegni, integrazioni salariali e trattenute, beni aziendali in possesso del dipendente (benefit e altro), dati sulla gestione e sulla valutazione delle attività lavorative, cariche pubbliche rivestite)*
Attività economiche, commerciali, finanziarie e assicurative *(dati contabili, ordini, buoni di spedizione, fatture, articoli, prodotti, servizi, contratti, accordi, transazioni, identificativi finanziari, redditi, beni patrimoniali, investimenti, passività, solvibilità, prestiti, mutui, ipoteche, crediti, indennità, benefici, concessioni, donazioni, sussidi, contributi, dati assicurativi, dati previdenziali)*
Istruzione e cultura *(curriculum di studi e accademico, pubblicazioni - articoli, monografie, relazioni, materiale audio-visivo, ecc - titoli di studio)*
Beni, proprietà, possessi *(proprietà, possessi e locazioni; beni e servizi forniti o ottenuti)*

Dati sul comportamento

(creazione di profili di utenti, consumatori, contribuenti, ecc; profili della personalità e dei tratti caratteriali)

Abitudini di vita o di consumo

(viaggi, spostamenti, preferenze o esigenze alimentari (eccettuate quelle fondate su convinzioni religiose o filosofiche), dati sull'appartenenza ad associazioni diverse da quelle di carattere religioso, filosofico, politico o sindacale, licenze, autorizzazioni (licenze di caccia o pesca, ecc); dati relativi ad attività sportive o agonistiche

- Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...)
- Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
- Dati di accesso e di identificazione (username, password, customer ID, altro…)
- Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)
- Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…)
- Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione
- Dati di profilazione
- Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
- Dati di localizzazione
- Dati che rivelino l'origine razziale o etnica
- Dati che rivelino opinioni politiche
- Dati che rivelino convinzioni religiose o filosofiche
- Dati che rivelino l'appartenenza sindacale
- Dati relativi alla vita sessuale o all'orientamento sessuale
- Dati relativi alla salute
- Dati genetici
- Dati biometrici

ENISA - Recommendations for a methodology of the assessment of severity of personal data breaches

- simple data

eg. biographical data, contact details, full name, data on education, family life, professional experience, etc

- behavioural data

location, traffic data, data on personal preferences and habits, etc.

- financial data

any type of financial data (e.g. income, financial transactions, bank statements, investments, credit cards, invoices, etc.). includes social welfare data related to financial information.

- sensitive data

any type of sensitive data (e.g. health, political affiliation, sexual life)

CNIL - EXEMPLE DE REGISTRE

- Etat civil, identité, données d'identification, images…
- Vie personnelle (habitudes de vie, situation familiale, etc.)
- Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, etc.)
- Données de connexion (adress IP, logs, etc.)
- Données de localisation (déplacements, données GPS, GSM, etc.)

Appendice B - Soggetti interessati

Garante per la protezione dei dati personali

Modello per la Notificazione del trattamento dei dati personali (artt. 7, 16 e 28 legge 31 dicembre 1996, n. 675)

- abbonati
- aderenti ad associazioni politiche, religiose o sindacali
- agenti e rappresentanti
- agricoltori
- artigiani
- candidati da considerare per l'instaurazione di un rapporto di lavoro
- clienti ed utenti
- commercianti
- consulenti e liberi professionisti, anche in forma associata
- consumatori
- detenuti o sottoposti a misure di sicurezza o di prevenzione
- familiari dell'interessato
- fornitori
- imprenditori e piccoli imprenditori
- lavoratori autonomi
- malati gravi o sottoposti a particolari cure
- pazienti
- personale dipendente
- personale pubblico dirigenziale e magistrati
- potenziali clienti
- scolari studenti di ogni ordine e grado
- soci, associati ed iscritti
- soggetti o organismi pubblici

Garante per la protezione dei dati personali

Tabella della procedura di notificazione D.lgs.196/03

- Amministratori, coordinatori o altre persone che ricoprono incarichi in organismi di tipo associativo.
- Assistiti
- Candidati a procedure concorsuali o selettive
- Candidati a procedure concorsuali o selettive- Cittadini di Paesi appartenenti all'U.E.
- Cittadini di Paesi appartenenti all'U.E.
- Cittadini di Paesi non appartenenti all'U.E.
- Cittadini italiani
- Clienti o utenti (anche potenziali)
- Concepiti e nascituri
- Condannati, detenuti o sottoposti a misure di sicurezza o prevenzione
- Coniugi e conviventi

- Consumatori
- Deceduti
- Donatori o riceventi
- Fedeli
- Genitori
- Gruppi familiari
- Gruppi omogenei per abitudini sessuali
- Gruppi omogenei per altre caratteristiche
- Gruppi omogenei per altre caratteristiche- Altro, specificare in dettaglio
- Gruppi omogenei per appartenenza razziale o etnica
- Gruppi omogenei per area geografica
- Gruppi omogenei per caratteristiche fisiche
- Gruppi omogenei per consanguineità
- Gruppi omogenei per fattori di rischio
- Gruppi omogenei per nazionalità
- Gruppi omogenei per provenienza geografica
- Imprenditori individuali, piccoli imprenditori o liberi professionisti
- Indagati o imputati
- Lavoratori o collaboratori
- Maggiori di età
- Malati gravi o sottoposti a particolari trattamenti di cura
- Militari o appartenenti alle forze dell'ordine
- Minori di età
- Neonati (entro il primo anno di vita)
- Parenti, affini o conviventi
- Passeggeri su veicoli o utenti di mezzi di trasporto
- Pazienti
- Pazienti, degenti o disabili
- Personale dipendente
- Persone affette
- Persone disabili
- Persone fisiche
- Persone in cerca di occupazione
- Scolari o studenti di ogni ordine e grado
- Soci o associati ad associazioni o fondazioni anche non riconosciute
- Soci, associati, aderenti o iscritti (anche potenziali o non facenti più parte dell'organismo di tipo associativo)
- Soci, associati, aderenti, iscritti e simpatizzanti (anche potenziali o non più facenti parte dell'organismo di tipo associativo)
- Soggetti con limitata capacità di intendere e volere
- Soggetti in difficoltà o pericolo
- Soggetti in difficoltà o pericolo (anche potenziali)
- Utenti di servizi o impianti sportivi

Appendice C - Finalità del trattamento

Garante per la protezione dei dati personali

Guida alla *Notificazione del trattamento dei dati personali (artt. 7, 16 e 28 legge 31 dicembre 1996, n. 675)*

Allegato b) - elenco delle finalità del trattamento

(le specificazioni riportate fra parentesi nelle voci seguenti vanno intese a titolo esemplificativo e non esaustivo)

FINALITÀ AMMINISTRATIVO-CONTABILI

Trattamento giuridico ed economico del personale

(calcolo e pagamento di retribuzioni ed emolumenti vari; applicazione della legislazione previdenziale ed assistenziale; cassa integrazione guadagni)

Gestione del personale

- reclutamento, selezione, valutazione e monitoraggio del personale
- concorsi interni
- test attitudinali
- formazione professionale
- collocazione personale dipendente all'esterno

Adempimento di obblighi fiscali o contabili

Adempimenti connessi al versamento delle quote di iscrizione a sindacati o all'esercizio di diritti sindacali

(gestione di permessi, distacchi, ...)

Igiene e sicurezza del lavoro

Programmazione delle attività

(pianificazione e monitoraggio dei compiti, del volume di lavoro e delle prestazioni lavorative)

Gestione del patrimonio mobiliare e immobiliare

Gestione della clientela

(amministrazione della clientela; amministrazione di contratti, ordini, spedizioni e fatture; controllo dell'affidabilità e solvibilità)

Gestione dei fornitori

(amministrazione dei fornitori; amministrazione di contratti, ordini, arrivi, fatture; selezioni in rapporto alle necessità dell'impresa)

Gestione del contenzioso

(*inadempimenti contrattuali; diffide; transazioni; recupero crediti; arbitrati; controversie giudiziarie)*

Servizi di controllo interno

(della sicurezza, della produttività, della qualità dei servizi, dell'integrità del patrimonio)

FINALITÀ CONNESSE AL SETTORE BANCARIO, CREDITIZIO, ASSICURATIVO, DI INTERMEDIAZIONE E DI CONSULENZA

Gestione contabile o di tesoreria

(amministrazione della contabilità individuale e della contabilità risparmi)

Servizi finanziari

(concessione e gestione di crediti, mutui e finanziamenti; indagini e valutazioni del rischio del credito, servizi di borsa; consulenza finanziaria, intermediazione finanziaria)

Strumenti di pagamento elettronico

(carte di credito e di debito; moneta elettronica)

Servizi assicurativi

(responsabilità civile, ramo vita, sanità e calamità)

Servizi di intermediazione

Attività di consulenza

Servizi a tutela di consumatori e utenti

FINALITÀ CONNESSE ALL'ATTIVITÀ COMMERCIALE

Vendita per corrispondenza o per telefono

(*offerta di beni e servizi attraverso mailing-list)*

Vendita per via telematica o radiotelevisiva

Commercializzazione di dati

(raccolta e trattamento di dati personali al fine della loro vendita o cessione)

Marketing

(analisi e indagini di mercato)

Pubblicità

Attività promozionali

Giochi o concorsi a premi

Rilevazione del grado di soddisfazione della clientela

FINALITÀ DI CARATTERE SANITARIO

Registrazione pazienti e gestione amministrativa

(monitoraggio ricoveri, registrazione dati sanitari a fini gestionali o di fatturazione)

Diagnosi, cura e terapia pazienti

(prevenzione, diagnosi e trattamento medico anche a mezzo di personale paramedico)

Monitoraggio di gruppi a rischio

Registrazione dei donatori

(creazione di archivi di donatori di sangue o di organi; interventi promozionali)

Interventi in caso di calamità, epidemie o malattie infettive

FINALITÀ DI CARATTERE SOCIALE

Servizi sociali e di assistenza

Attività di previdenza

Attività di volontariato

Attività di solidarietà e beneficenza

Attività politica

Attività sindacale

FINALITÀ DI RICERCA

Ricerche epidemiologiche

(analisi su specifici fattori o eventi; esposizione a rischi sanitari; consumi; morbilità e mortalità)

Ricerche biomediche

(ricerche sull'eziologia di patologie mediche e gli effetti di terapie mediche; indagini cliniche)

Ricerche sociologiche e di opinione

(studi su opinioni e comportamenti umani, interazioni interpersonali e organizzazione della società)

Ricerche storiche

Analisi statistiche e psicometriche

FINALITÀ DI INFORMAZIONE, ISTRUZIONE, CULTURA E VALORIZZAZIONE DEL TEMPO LIBERO

Informazione radio-televisiva

Informazione per via telematica

Quotidiani, periodici ed altre pubblicazioni

Libri ed altre attività editoriali

Informazione scientifica o giuridica

Istruzione ed assistenza scolastica

(amministrazione di scolari e studenti, organizzazione delle attività di insegnamento e valutazione; assistenza, anche a fini di orientamento professionale, sussidi, borse, assegni, ...)

Istruzione ed assistenza universitaria

(amministrazione degli studenti, organizzazione delle attività di insegnamento e valutazione; assistenza, anche a fini di orientamento professionale, sussidi, borse, assegni, ...)

Attività artistiche e culturali

Attività turistiche e ricreative

Attività sportive

FINALITÀ DI GENERE DIVERSO DA QUELLE DESCRITTE IN PRECEDENZA

Amministrazione della popolazione

(gestione delle anagrafi della popolazione e dei registri dello stato civile; rilascio di certificati ed estratti)

Attività di carattere elettorale

(tenuta liste elettorali; svolgimento di compiti pubblici relativi a consultazioni elettorali e referendarie)

Organizzazione di campagne elettorali

(raccolta di fondi e di nominativi di sostenitori; gestione di incontri; pubblicità a domicilio, telefonica o telematica)

Amministrazione degli stranieri

(rilascio di permessi e visti; riconoscimento di titoli e diplomi; svolgimento di altri compiti in materia di immigrazione)

Attività istituzionali in ambito comunitario e internazionale

(affari comunitari; trattati; cooperazione comunitaria e internazionale; commercio con l'estero; accordi di amicizia e collaborazione)

Attività istituzionale delle forze armate o per la difesa e la sicurezza dello Stato

Ordine e sicurezza pubblica

(misure di sicurezza; prevenzione, accertamento e repressione dei reati)

Amministrazione della giustizia

(procedimenti giudiziari civili, penali, amministrativi e tributari)

Gestione e controllo di istituti penitenziari

Protezione civile

(interventi per disastri e calamità; assistenza; gestione sussidi e interventi di recupero; rapporti con il volontariato)

Difesa del suolo, tutela dell'ambiente e della sicurezza della popolazione
(radioprotezione, campi magnetici)
Pianificazione urbanistica, amministrazione del territorio, controlli su illeciti edilizi
Progettazione, affidamento o esecuzione di opere pubbliche
Autorizzazioni, concessioni, permessi, licenze e nulla-osta
(adozione dei provvedimenti di rilascio e attività connesse; individuazione degli aventi diritto, verifica e controllo delle condizioni)
Vigilanza e controllo sistema monetario e valutario
Attività e controlli doganali
Accertamento e riscossione di tasse e imposte
Finanziamenti, sussidi e sovvenzioni
(concessione di finanziamenti, sussidi e sovvenzioni: individuazione degli aventi diritto, calcolo, monitoraggio)
Documentazione di beni e patrimoni
(tenuta di registri di beni mobili e immobili; archivi catastali; rilascio di certificazioni e attestazioni)
Operazioni di trasporto
(passeggeri e merci)
Prenotazione di servizi ed emissione biglietti
(iniziative sportive, culturali, ricreative, ...)
Relazioni con il pubblico
Gestione di elenchi, attività e contributi di soci, sostenitori o associati
(persone fisiche, giuridiche, associazioni, fondazioni, comitati, ...)

Appendice D - Elenco documenti

OBBLIGATORI: Ben definiti ed il cui contenuto è specificatamente declinato

- informative
- formula del consenso
- contratti di designazione dei responsabili
- contratti di designazione dei sub responsabili
- contratti o altri atti per contitolarità, rappresentanza…
- designazione amministratori di sistema
- designazione del DPO
- istruzioni per i soggetti che operano sotto l'autorità del Titolare o del Responsabile
- regolamentazione del trasferimento dei dati all'estero
- registri delle attività di trattamento
- registro delle violazioni
- notifica di violazione all'Autorità Garante
- comunicazione di violazione agli interessati
- DPIA
- Norme vincolanti d'impresa
- Comunicazione preventiva all'Autorità Garante (art. 36)

NECESSARI: Implicitamente previsti

- registro delle richieste degli interessati
- modulistica per rispondere agli interessati
- analisi del rischio ai sensi dell'art. 24
- analisi del rischio ai sensi dell'art. 25
- analisi del rischio ai sensi dell'art. 32
- regolamentazione del rapporto con altri Titolari
- regolamentazione del rapporto con altri soggetti che accedono ai locali in cui si svolgono trattamenti
- deleghe di rappresentanza del Titolare
- attestazione della mancata necessità di designare un DPO
- elenco analitico dei soggetti interessati
- elenco analitico dei soggetti esterni (Titolari, responsabili…)
- elenco analitico dei soggetti che operano sotto l'autorità del Titolare (o del Responsabile)
- elenco delle misure tecnico/organizzative implementate ai sensi degli artt. 24, 25, 32

ACCESSORI: Implicitamente richiesti al fine di essere in grado di dimostrare la propria conformità al GDPR

- mappatura dell'organizzazione
- policy e procedure
- documentazione tecnica e funzionale in ambito IT
- log
- rilevazione di eventi che attivano l'art. 25.1
- verifiche ispettive

POLICY E PROCEDURE (MACRO AMBITI)

Rilevazione ed analisi della normativa che impattano sul modello privacy
Rilevazione di eventi endo/eso aziendali che impattano sul modello privacy
Definizione e rilascio delle informative
Definizione base giuridica del trattamento
Modalità di raccolta e gestione del consenso
Gestione dei diritti degli interessati
Gestione dei principi (qualità dei dati, tempi di conservazione…)
Valutazione dei ruoli dei soggetti esterni
Valutazione delle caratteristiche dei soggetti esterni ai quali si affidano trattamenti
Valutazione della necessità o meno di un DPO
Valutazione del DPO
Valutazione del rispetto delle condizioni in merito ai trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali
Valutazione delle misure tecniche ed organizzative per il rispetto dell'art. 5 (Principi)
Valutazione delle misure di sicurezza
Metodologie per le analisi dei rischi
Metodologia per l'esecuzione di una DPIA
Metodologia per l'esecuzione di un'analisi privacy by design e by default
Metodologia per la rilevazione di un incidente di sicurezza
Metodologia per la gestione di un incidente di sicurezza
Metodologia per la valutazione di una violazione di dati personali
Metodologia per la pianificazione, esecuzione e valutazione delle verifiche ispettive
Selezione, valutazione, implementazione, monitoraggio delle misure di sicurezza
Istruzioni per i soggetti autorizzati a effettuare i trattamenti

Appendice E – Buone pratiche per i Registri delle attività di trattamento[1]

https://www.cnil.fr/sites/default/files/atoms/files/registre-rgpd-cnil_decembre-2019.pdf

Council: https://www.consilium.europa.eu/en/general-secretariat/corporate-policies/data-protection/search/

EEAS: via https://eeas.europa.eu/headquarters/headquarters-homepage/3032/data-protection_en

SRB: ttps://srb.europa.eu/sites/srbsite/files/srb_public_register_of_records_0419pdf.pdf

ESMA: https://www.esma.europa.eu/records-register

EEA: https://www.eea.europa.eu/about-us/data-protection/central-register-of-records-of

EASA: https://www.easa.europa.eu/data-protection

EACEA: https://eacea.ec.europa.eu/about-eacea/document-register-eacea/public-register-processing-activities_en

eu-LISA: https://www.eulisa.europa.eu/AboutUs/DP/Documents/web_DPO_Register.pdf

EDPS: https://edps.europa.eu/about/data-protection-within-edps/records-register_en

ACER: https://www.acer.europa.eu/en/The_agency/Data-Protection/_layouts/15/WopiFrame.aspx?sourcedoc=%7bf583e2d7-681a-49a3-b2fb-2db0ce1db9df%7d&action=edit&source=https%3a//www.acer.europa.eu/en/The_agency/Data-Protection/Documents/Forms/AllItems.aspx

S2R JU: https://shift2rail.org/dpregister/

EU-OSHA: https://osha.europa.eu/en/about-eu-osha/data-protection/register-records

1 In base all'art. 31 del Regolamento 2018/1725, sostanzialmente analogo all'art. 31 del GDPR

Appendice F – Metodologie, moduli, strumenti ufficiali

METODOLOGIE E MODELLI

Analisi dei rischi

ENISA

- Handbook on Security of Personal Data Processing
- Guideliness for SMEs on the securirty of personal data processing

CNIL

- *Parte sull'analisi dei rischi nella metodologia della DPIA*

AEPD

- Guia práctica de Análisis de riesgos en los tratamientos de datos personales sujetos al RGPD
- Listado de cumplimiento normativo

DPIA

CNIL

- Analyse d'impact relative à la protection des données (AIPD) 1: la méthode
- Analyse d'impact relative à la protection des données (AIPD) 2: les modèles
- Analyse d'impact relative à la protection des données (AIPD) 3: les bases de connaissances

AEPD

- Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD
- Modelo de informe de evaluación de impacto en la protección de datos (eipd) para el sector privado
- Modelo de informe de evaluación de impacto en la protección de datos (eipd) para administraciones públicas

MISURE DI SICUREZZA

ENISA

- Handbook on Security of Personal Data Processing
- Guideliness for SMEs on the securirty of personal data processing
- Reinforcing trust and security in the area of electronic communications and online services - Sketching the notion of "state-of-the-art" for SMEs in security of personal data processing

CNIL

- La sécurité des données personnelles

DESIGNAZIONE DEL RESPONSABILE DEL TRATTAMENTO

AEPD

- Directrices para la elaboration de contratos entre responsables y encargados de tratamiento

CNIL

- Règlement européen sur la protection des données personnelles - Guide du sous-traitant - Edition septembre 2017
- Sous-traitance: Exemple de clauses
- Proposition de clause de confidentialité en cas de sous-traitance *(pre GDPR)*
- Proposition de clause de confidentialite en cas d'operations de maintenance ou de telemaintenance dans le cadre d'une sous-traitance *(pre GDPR)*

DESIGNAZIONE DEL DPO

Autorità Garante sulla protezione dei dati personali

- Schema di atto di designazione del Responsabile della Protezione dei Dati
  - https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7322273

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

CNIL

- Registre des activités de traitement de la cnil
  - https://www.cnil.fr/sites/default/files/atoms/files/registre-rgpd-cnil_decembre-2019.pdf
- RGPD - Modèle de registre (pdf)
  - https://www.cnil.fr/sites/default/files/atoms/files/registre_rgpd_basique.pdf

Autorità Garante sulla protezione dei dati personali

- Modello di "registro semplificato" delle attività di trattamento del titolare per PMI (ALLEGATO 1)
  - https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9048342
- Modello di "registro semplificato" delle attività di trattamento del responsabile per PMI (ALLEGATO 2)
  - https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9048395

INFORMATIVA

AEPD

- Guía para el cumplimento del deber de informar

VERIFICHE ISPETTIVE

AEPD

- Listado de cumplimiento normativo

EDPB

- Linee guida 1/2018 relative alla certificazione e all'identificazione di criteri di certificazione in conformità degli articoli 42 e 43 del regolamento (UE) 2016/679 – Allegato 2

DPCI

- Preparing your organisation for the general data protection regulation

ICO

- Auditing data protection a guide to ICO data protection audits *(pre GDPR)*

CODICI DI CONDOTTA

AEDP

- Códigos de conducta inscritos
    - https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/codigos-de-conducta/codigos-inscritos

Autorità Garante sulla protezione dei dati personali

- Codici di condotta
    - https://www.garanteprivacy.it/codici-di-condotta

CERTIFICAZIONE DEL PERSONALE (non previsto dal GDPR)

AEPD

- Certification scheme of data protection officers from the spanish data protection agency (dpo-aepd scheme).

CNIL

- Délibération n° 2018-317 du 20 septembre 2018 portant adoption des critères du référentiel d'agrément d'organismes de certification pour la certification des compétences du délégué à la protection des données (DPO)

STRUMENTI

GESTIONE GDPR

AEPD

- Facilita RGPD
    - https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd
- Facilita EMPRENDE
    - https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-emprende

ANALISI DEI RISCHI

ENISA

- https://www.enisa.europa.eu/news/enisa-news/securing-personal-data-a-risky-business

DPIA

CNIL

- https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

AEPD

- https://gestiona.aepd.es/

VIOLAZIONI DATI PERSONALI

ENISA

- Personal data breach notification tool
  - https://www.enisa.europa.eu/topics/data-protection/personal-data-breaches/personal-data-breach-notification-tool

ASSESSMENT

ICO

- **Data** protection **self assessment**
  - https://ico.org.uk/for-organisations/data-protection-self-assessment/

ESEMPI DI GUIDE

ICO

- Guide to General Data Protection Regulation (GDPR)
- The Guide to Freedom of Information
- Overview of the General Data Protection Regulation (GDPR)
- The Guide to Data Protection

CNIL

- Guide pratiqué de sensibilisation au RGPD

AEPD

- Guía del Reglamento General de Protección de Datos para responsables de tratamiento
- Guide on personal data breach management and notification
- A Guide to Privacy by Design
- Protección de Datos: Guía para el Ciudadano

Autorità Garante sulla protezione dei dati personali

- Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali

- Manuale per supportare i Responsabili della Protezione dei dati (RPD) dei soggetti pubblici nell'applicazione del Regolamento Ue 2016/679

Appendice G – Metodologie, moduli, strumenti non ufficiali

PRIVACY BY DESIGN

INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

- Privacy by design …take the challenge

MODELLI

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA

- Privacy Toolkit

NEW ZEALAND GOVERNMENT

- Realising opportunities with personal information in a privacy friendly way

OASIS

- Privacy Management Reference Model And Methodology (PMRM) Version 1.0

AUSTRALIAN INFORMATION COMMISSIONER

- Australian Privacy Principles guidelines

FRAMEWORK

AICPA CICA

- Generally Accepted Privacy Principles

OECD

- The OECD privacy framework

APEC

- APEC Privacy Framework

NIST

- NIST Privacy Framework

AAVV

- Framework Nazionale per la Cybersecurity e la Data Protection

POLICY DI SICUREZZA

- **AUSTRALIAN GOVERNMENT INFORMATION SECURITY MANUAL**
  - Reinforcing trust and security in the area of electronic communications and online services - Sketching the notion of “state-of-the-art” for SMEs in security of personal data processing
- **SECURITY POLICY TEMPLATES**
  - https://www.sans.org/security-resources/policies

MISURE DI SICUREZZA

AAVV

- Cybersecurity framework nazionale

BSI

- It-Grundschutz Catalogues

NIST

- Special publication 800-53 (rev. 4)

CODICI DI CONDOTTA

CISPE

- Data Protection - Code of Conduct for Cloud Infrastructure Service Providers

Cloud Security Alliance (CSA)

- Code of conduct for GDPR compliance Data Protection