CompuSoft
PRODUZIONE SOFTWARE

SOFTWARE GESTIONALE – APPLICATIVI SU COMMISSIONE
CONSULENZE INFORMATICHE – PROGRAMMAZIONE WEB

GDPR

General Data Protection Regulation
Regolamento UE 2016/679
Regolamento Europeo in materia di protezione dei dati personali.

MAPPA DELLE SLIDES

SLIDE N. 1 - Presentazione

La finalità del regolamento è quella di proteggere i diritti delle persone alla riservatezza dei dati, impedendo che vengano trattati per motivi illeciti e senza il consenso degli interessati. Art. 1, 5, 6

L'adeguamento alla norma è un onere ed una opportunità.

Un onere perché sono necessari adempimenti burocratici e vengono affrontati dei costi.

Ma l'adeguamento è anche una opportunità perché aumenta la nostra sensibilità ai problemi della sicurezza che sono sempre più pressanti e che possono rappresentare un grave costo se si viene coinvolti in episodi di crimine informatico.

SLIDE N. 2 - A chi interessa

L'approccio che teniamo in questa trattazione è orientato a venire incontro alle esigenze più comuni delle aziende a cui ci rivolgiamo.

Ci orientiamo verso un approccio pratico che si focalizza sulle parti della normativa maggiormente rilevanti per motivi burocratici e funzionali.

In fase di trattazione, sarà necessario indagare la necessità di approfondire aspetti meno comuni e particolari.

COMPUSOFT di DRIUSSI CLAUDIO – VIA DAMIANO CHIESA, 33/B – 33170 PORDENONE
TEL 0434.523012 - P.IVA 01231280932 – C.F. DRSCLD56M29F750D – http://compusoft.it - info@ compusoft.it

SLIDE N. 3 – Un po' di definizioni

L'Art. 4 del regolamento spiega alcuni dei termini che vengono utilizzati. Alcuni sono più importanti di altri, i principali sono quelli esposti.

Il dato personale è qualsiasi informazione che riguarda una persona.

L'interessato è la persona di cui vengono trattati i dati personali.

Il trattamento è la serie di operazioni coordinate effettuate sui dati personali.

Il Titolare è colui che effettua il trattamento.

Il responsabile viene nominato dal titolare per gestire il trattamento. Art. 28

L'addetto viene incaricato dal responsabile a trattare i dati. L'addetto non viene esplicitamente identificato dalla norma, ma nell'Art. 28 si indica che le persone che operano sul trattamento hanno un obbligo di riservatezza.

Il responsabile esterno è un soggetto terzo che tratta particolari aspetti dei dati, Art. 28, ad esempio sono responsabili esterni i tecnici informatici che fanno la manutenzione dei sistemi, oppure i studi commercialisti.

Il destinatario dei dati è un soggetto a cui vengono comunicati i dati nell'ambito del trattamento, ad esempio banche, trasportatori ecc…

SLIDE N. 4 - Diritti degli interessati

La normativa è volta a tutelare diritti. I diritti vengono trattati dall'art. 12 al art. 22

In linea generale l'interessato dovrà essere a conoscenza che viene fatto un trattamento che lo riguarda, dovrà ottenere tutte le informazioni sui dati trattati, sui modi e su eventuali destinatari.

Potrà richiedere la rettifica di dati non esatti ed eventualmente la loro cancellazione se non esistono impedimenti di natura legale o contrattuale.

Infine si potrà opporre al trattamento qualora esso venisse fatto in modo automatico.

Le aziende sono obbligate per legge a conservare i documenti contabili per 5 anni per

motivi fiscali e 10 per motivi legali. Pertanto se sono state emesse fatture non è possibile fare cancellazioni prima di 10 anni.

Se invece sono stati fatti solo preventivi e registrazioni riguardanti pubblicità e marketing, su richiesta dell'interessato si dovrà procedere alla cancellazione.

In tutti i casi comunque si dovrà procedere ad informare gli interessati.

SLIDE N. 5 - Le aziende non sono tutte uguali

I trattamenti sono operazioni compiute sui dati personali. Art. 4 Anche se non specificato nel regolamento, conviene suddividere i trattamenti in modo funzionale in base alla finalità ed alle persone coinvolte nel trattamento.

I trattamenti circoscritti, vengono svolti in formato elettronico e cartaceo esclusivamente all'interno dell'azienda o al massimo mediante collegamenti punto a punto.

Con trattamenti cloud intendiamo trattamenti che fanno uso di tecnologie internet come ad esempio Applicativi web utilizzati solo da personale addetto, sistemi che acquisiscono dati personali in modo automatico ad esempio siti di commercio elettronico e sistemi di profilazione, ad esempio tecnologie cookies, social network ecc...

La distinzione è importante perché cambiano radicalmente le misure che si di sicurezza che devono essere adottate. Nel caso dei trattamenti circoscritti si devono adottare le misure di sicurezza informatiche comuni per le aziende ed è opportuno formare il personale in modo adeguato soprattutto per l'uso della posta elettronica e dell'uso in genere dei PC. Nel caso di trattamenti internet invece, il rischio di attacchi da perte di criminali informatici è una seria minaccia che non va sottovalutata e che richiedere misure quali la cifratura dei dati e l'anonimizzazione dei dati personali.

SLIDE N. 6 - I trattamenti non sono tutti uguali

I trattamenti aziendali comuni sono quelli utilizzati dalle aziende per la gestione ordinaria. Ad esempio Amministrazione contabile, gestione dei dipendenti, gestione del ciclo attivo di produzione e vendita, gestione del marketing.

I trattamenti speciali, sono quelli che esulano dalla gestione ordinaria. Ad esempio cartelle cliniche, trattamenti di profilazione ed in genere quelli che sono di per se stessi l'oggetto del ciclo di produzione.

SLIDE N. 7 - I dati non sono tutti uguali

I dati personali comuni sono quelli in grado di identificare le persone, possono essere trattati se indispensabili per il trattamento ad esempio per emettere le fatture serve la Partita IVA o il codice fiscale, ma non il colore dei capelli o degli occhi. Invece un parrucchiere ha bisogno di conoscere il colore dei capelli per proporre le tinte ai suoi clienti. Art. 5

I dati personali particolari sono quelli che contengono informazioni sulla razza, religione, opinioni politiche, dati biometrici e vita sessuale, per i quali è necessario il consenso esplicito al trattamento, Art. 9

I dati possono avere rilevanza diversa a seconda del tipo di trattamento. In alcuni casi il trattamento è sensibile anche su dati comuni, ad esempio quando vengono fatte profilazioni che possono portare a deduzioni non esplicite. Ad esempio il tracciamento dei movimenti GPS può portare a deduzioni sulle abitudini delle persone. Viceversa informazioni particolari possono avere scarsa rilevanza se il trattamento non è protratto nel tempo ed eseguito senza l'ausilio di sistemi elettronici.

SLIDE N. 8 - Cosa devono fare le aziende

Viene consigliato a tutti di tendere il "Registro dei trattamenti" Art. 30

Il titolare del trattamento deve attivare comportamenti virtuosi tenendo conto delle innovazioni tecnologiche e dei costi di applicazione per fare in modo che i sistemi siano progettati in modo sicuro e che la riservatezza dei dati abbia la precedenza sugli altri aspetti.

Per i trattamenti in essere è necessario adottare tecniche di adeguamento. Art. 25

L'informativa deve essere sintetica e facilmente comprensibile, ma deve contenere tutte le informazioni richieste dalla norma. Art. 13

Nel caso di trattamenti automatici o di dati personali è richiesto il consenso esplicito al trattamento.

Spesso i per eseguire i trattamenti è necessario che i dati vengano comunicati a destinatari terzi. Ad esempio banche, studi legali, trasportatori, sub fornitori, consulenti esterni, pubbliche amministrazioni ed altri. Sarà opportuno accertarsi che anche questi trattino i dati in modo conforme al regolamento.

SLIDE N. 9 - Come devono operare le aziende

In realtà il processo è più articolato, ma la semplificazione aiuta ad adottare una strategia efficace.

Il censimento dei trattamenti serve ad individuare i trattamenti che vengono eseguiti ma anche la loro liceità. Art. 5. Vengono anche individuati il Responsabile e gli addetti Art. 28 e vengono predisposte le informative Art. 13

L'analisi dei rischi, anche chiamata "Valutazione d'impatto" serve per individuare le problematiche di sicurezza che non coinvolgono solo la divulgazione dei dati, ma anche la loro distruzione e questo può rappresentare un danno notevole per il patrimonio aziendale.

Il rischio deve essere valutato tenendo conto della probabilità che accadano eventi avversi, del tipo di dati trattati e della natura del trattamento. Esistono eventi gravissimi che hanno una probabilità molto bassa ed eventi che invece capitano molto spesso ma che si possono prevenire facilmente.

Dopo aver individuato i rischi si devono mettere in atto misure adeguate per la prevenzione dei rischi. Ciò che è adeguato non lo stabilisce il regolamento, ma viene giudicato dal titolare secondo il principio di responsabilizzazione (Accoutability). Lo scopo è quello di tendere a fare in modo che i trattamenti rispettino i principi di Privacy by Design e Privacy by Default. L'adeguamento non viene fatto una volta per tutte,

Alla fine, anche se non obbligatorio per tutti i soggetti, si consiglia di redigere un "Registro dei trattamenti" Art. 30 che contiene tutte le informazioni richieste dal regolamento, si devono anche preparare i contratti di nomina dei responsabili dei trattamenti ed è opportuno preparare lettere di incarico per gli addetti che operano sui dati e richieste di consenso per dipendenti ed eventuali interessati di cui si trattano dati particolari.

Il processo di adeguamento non si esaurisce con la stesura della documentazione, ma è un processo continuo che individua eventuali nuovi trattamenti, nuovi rischi e che mette in atto nuove misure di adeguamento.

Sarà quindi necessario tenere sempre aggiornata la documentazione che verrà ristampata in caso di necessità.

SLIDE N. 10 - Obblighi e Sanzioni

La norma è in vigore dal 2016, ma dal 25 maggio 2018 entra in vigore le sanzioni.

Eventuali violazioni dovranno essere comunicate al Garante e direttamente agli interessati

entro 72 ore dal momento in cui se ne viene a conoscenza, esistono però alcune deroghe a questa regola.

Le sanzioni sono severe perché sono pensate per frenare la profilazione su larga scala di imprese di grandi dimensioni (social network), però sono un arma potente nelle mani degli organismi di controllo.

L'organismo che tutela il rispetto della normativa è il Garante della Privacy, ma non si sa ancora chiaramente chi sarà ad effettuare i controlli, probabilmente la Polizia postale e/o la Guardia di Finanza.

Al momento non ci sono comunicazioni ufficiali di deroghe dalla data stabilita. Alcuni ritengono che ci siano indicazioni di una moratoria fino a fine 2018, però in mancanza di ufficialità è comunque attivo il sistema sanzionatorio a partire dalla data indicata.

SLIDE N. 11 - Argomenti particolari

Il GDPR contiene prescrizioni e concetti che spesso sono poco importanti per la maggior parte delle aziende obbligate al suo rispetto. Ne elenchiamo alcune:

Portabilità dei dati: In caso di richiesta l'interessato ha diritto ad ottenere i dati che lo riguardano in un formato elettronico facilmente utilizzabile. Ad esempio documenti PDF oppure tabelle elettroniche nei formati più comuni.

DPO: Oltre alla figura del responsabile del trattamento, in caso di aziende sopra i 250 dipendenti o per la pubblica amministrazione o infine se vengono effettuati trattamenti sistematici e larga scala è obbligatoria la nomina del "Responsabile della protezione dei dati" anche chiamato DPO il cui compito è quello di fare da tramite con il Garante e di accertarsi che l'obiettivo della tutela dei dati venga perseguito e raggiunto.

Per trattamenti su larga scala si intende con numero elevato di interessati, potenzialmente identificabili come ad esempio la videosorveglianza sui mezzi pubblici. I trattamenti sistematici invece possono essere sistemi di videosorveglianza, oppure di geolocalizzazione su app o anche sistemi di profilazione.

Paesi Extra UE: Solitamente le aziende non fanno trattamento dei dati in paesi al di fuori della UE, con eccezione forse della domiciliazione fisica di siti Web. Le prescrizioni sul trattamento di dati in Paesi terzi sono piuttosto severe e stringenti ma riguardano solo i soggetti interessati.

Pseudonimizzazione e Cifratura: Nel caso di trattamenti che fanno uso della rete internet, è necessario adottare misure atte a prevenire i crimini informatici, anche con le tecniche di

cui sopra.

Garante della Privacy: l'organo preposto in Italia alla tutela dei dati personali è il Garante della Privacy il quale oltre ad avere il potere sanzionatorio ha anche il compito di assistere i soggetti per aiutarli ad adeguarsi.

In particolare esistono casi in cui è richiesta la valutazione di impatto ad esempio per trattamenti su larga scala, oppure per sistemi di vigilanza, in tali casi è necessario chiedere il parere del garante per sapere se è possibile tenere il trattamento ed il Garante può anche negare il consenso.

Codici di condotta: Il Garante favorisce l'adozione di regolamenti specifici per particolari categorie, ad esempio per quanto riguarda le attività di giornalismo e di diritto alla informazione, ma in generale ogni volta che una categoria ritiene di dover adottare comportamenti comuni.

SLIDE N. 12 - Approfondimenti

Troviamo utile approfondire qualche argomento direttamente o indirettamente correlato al GDPR

SLIDE N. 13 - Tipi comuni di trattamento

La gestione amministrativa e contabile parte dal momento della emissione della fattura e della registrazione delle fatture di acquisto. E' un trattamento obbligatorio con vincoli di legge e coinvolge diversi destinatari, ad esempio studi commercialisti, banche, legali, consulenti ecc.

L'attività di produzione e vendita può variare moltissimo da azienda ed azienda ed esistono molte variazioni anche in merito ad eventuali suddivisioni in più trattamenti ad esempio le industrie che producono beni materiali hanno problematiche relative al ciclo produttivo ed il coinvolgimento di sub forniture ed approvigionamenti. Le aziende che producono servizi hanno la gestione di "Commesse" per specifici clienti. La vendita al pubblico ha la gestione delle garanzie e delle fidelizzazioni e così via. Questi trattamenti vanno valutati di caso in caso.

La promozione commerciale viene svolta da molte aziende, ma non da tutte. In questo caso si deve tener conto dei destinatari di promozione che possono essere clienti acquisiti oppure clienti potenziali, poi si deve considerare l'uso di ausili informatici come ad esempio i programmi di CRM.

Anche la gestione del personale dipendente è un trattamento obbligatorio, ma in questo caso si trattano dati particolari, perché possono essere coinvolti dati che riguardano la salute oppure opinioni politiche ed appartenenze religiose, per questo motivo è necessario adottare le misure prescritte per questo tipo di dato. Normalmente i dati vengono trattati dai consulenti del lavoro e le aziende ricevono semplicemente le buste paga tramite email. In questo caso il consiglio più semplice è di cancellare le mail ricevute e di memorizzare i dati delle buste paga in chiavi usb conservare a parte e possibilmente crittografate.

Le attività connesse ad internet possono essere le più svariate. Le più comuni sono la gestione del commercio elettronico, la gestione di blog e la condivisione di documenti. Data la variabilità dei sistemi impiegati, per questi casi è sempre necessaria l'assistenza dei consulenti tecnici informatici che ci forniscono il servizio.

SLIDE N. 14 - La videosorveglianza

Spesso le aziende adottano sistemi di videosorveglianza. Il garante ritiene che il sistema è a norma quando rispetta i seguenti principi:

Liceità: il principio permette la registrazione delle immagini se sono necessarie ad obblighi di legge o per tutelare un legittimo interesse.

Necessità: secondo questo principio le riprese devono limitarsi solamente a ciò che è necessario per raggiungere gli scopi prefissati.

Proporzionalità: secondo questo principio, gli impianti di videosorveglianza vanno impiegati solo in luoghi dove è realmente necessario, limitando le riprese alle sole aree interessate escludendo la visuale su quelle circostanti.

Finalità: gli scopi della videosorveglianza devono essere espliciti e legittimi, e limitati alle finalità di pertinenza del titolare dei dati.

Si possono conservare i dati per 24 ore con alcune deroghe ad esempio per gli istituti di credito o in caso di richieste specifiche.

Deve essere presente un cartello chiaramente visibile e disposto al di fuori del campo visivo che informa i visitatori e non si può usare la videosorveglianza per controllare il lavoro dei dipendenti.

Le apparecchiature dovrebbero registrare i dati internamente senza comunicare i dati via internet, in caso contrario ci si deve accertare che chi fornisce il servizio abbia i server in Europa e che rispetti la legge.

Se si escludono trattamenti speciali, non sono richieste comunicazioni esplicite al garante per l'uso di sistemi di videosorveglianza.

SLIDE N. 15 - Regole comuni di sicurezza

Per i trattamenti circoscritti all'interno dell'azienda e per la buona gestione della sicurezza consigliamo di attivare alcune regole comuni di sicurezza.

In particolare, tenere sempre aggiornati i programmi ed i sistemi operativi aiuta a difendersi da rischi conosciuti. I log di accessi e firewall aiutano a scoprire se sono in essere tentativi di accatto informatico. La robustezza delle password e la formazione del personale limitano i rischi dovuti al fattore umano che solo spesso l'anello debole della sicurezza.

Soprattutto è fondamentale avere buoni sistemi di backup con criteri di separatezza e di isolamento. Ed è necessario controllare frequentemente che i dati siano effettivamente copiati in modo corretto e ripristinabili.

SLIDE N. 16 - Qualche parola sui siti web

Molte aziende dispongono di siti vetrina, alcuni offrono servizi personalizzati alla clientela come ad esempio la disponibilità di documenti riservati, altri infine offrono servizi di commercio elettronico.

Per tutti consigliamo ove possibile di attivare il protocollo per le comunicazioni cifrate https che oggi è più facilmente ottenibile rispetto al passato.

Poi è importante che le aree riservate dei siti siano protette con password robuste e sistemi di prevenzione degli attacchi di forza bruta. I più diffusi ambienti per siti come ad esempio Wordpress, Joomla, Drupal ed altri, spesso dispongono di componenti per la sicurezza efficaci.

Infine per i siti che offrono servizi di commercio elettronico con meccanismi di autenticazione automatica, è necessario che vengano rispettate le prescrizioni del regolamento in particolare con la richiesta di accettazione esplicita del trattamento. Questo non serve se gli utenti non hanno la facoltà di autenticarsi autonomamente ma solo su invito con comunicazione delle credenziali da parte del titolare.

Quasi tutti i siti contengono form per la richiesta di informazioni, anche in questo caso è necessario mettere una spunta di accettazione per il trattamento.

SLIDE N. 17 – I servizi di internet

Esistono servizi gratuiti ed a pagamento per la condivisione di dati molto diffusi che di solito sono forniti dai giganti americani di internet. Sono servizi distribuiti di cui è difficile individuare la localizzazione dei server ed anche le regole di riservatezza spesso non sono adeguate alla normativa europea.

Se possibile, si consiglia di usare servizi alternativi. Ad esempio per la posta elettronica, invece di usare Gmail o Hotmail, è meglio usare caselle con un proprio dominio fornite da provider europei, oppure per i servizi cloud di domiciliazione dei dati si possono utilizzare soluzioni alternative disponibili come NextCloud.

Si possono invece utilizzare servizi di promozione social come ad esempio pagine personali su Facebook o su Google Plus, facendo attenzione però a non coinvolgere dati personali di terzi senza autorizzazione.

ORIENTAMENTO ALLA LETTURA DEL GDPR

Il GDPR è un documento scritto in legalese di 88 pagine. La lettura può risultare difficile se non si ha una conoscenza specifica dell'argomento o se non si ha esperienza nella lettura di documenti legali.

https://www.privacyitalia.eu/testo-del-gdpr-pdf-italiano/4746/

Per facilitare l'orientamento in caso di necessità di approfondimento, consigliamo di leggere la versione annotata fornita dal Garante che almeno contiene un indice e porta alcuni riferimenti tra la prima e la seconda parte.

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6264597

Il Garante mette anche a disposizione un breve testo contenente le informazioni più rilevanti e le differenze rispetto alla normativa precedente.

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6807118

In ogni caso proponiamo un breve riassunto utile per facilitare la ricerca delle informazioni.

Il documento si compone di due parti. Nella prima parte si trovano le considerazioni (considerando) che hanno motivato la stesura del regolamento e nella seconda vengono esposti gli articoli che recepiscono le considerazioni.

Le considerazioni si articolano in 173 punti che secondo noi vanno lette solo in caso di ricerche avanzate specifiche e con l'aiuto dei riferimenti presenti nel documento proposto dal Garante.

La seconda parte contiene gli articoli vincolanti. I primi articoli mediamente contengono informazioni di tipo generale, andando avanti si arriva ad argomenti piu specifici che non sempre coinvolgono un numero vasto di soggetti.

Gli articoli sono raggruppati in questo modo:

Capo I - Disposizioni generali

Art. da 1 a 4

Si tratta l'ambito di applicazione e delle definizioni

Capo II - Principi

Art. da 5 a 11

Si parla di liceità del trattamto, condizioni per il consenso, minori, tipi particolari di dati (sensibili), giudiziari, trattamenti senza identificazione.

Capo III - Diritti

vengono delineati i diritti degli interessati

Sezione 1 - trasparenza art. 12

Sussiste l'obbligo di informare gli interessati sul esercizio dei propri diritti

Sezione 2 - informazione ed accesso ai dati art. 13 - 15

Viene indicato ciò che deve essere contenuto nella "informativa" che è un obbligo formale.

Sezione 3 - rettifica e cancellazione art. 16 - 20

L'interessato ha il diritto che i dati possano essere rettificati, cancellati, ha il diritto di limitare il trattamento e di essere notificato in caso di variazioni ed infine ha il diritto di ricevere copia dei dati.

Sezione 4 - diritto di opposizione al trattamento automatico art. 21 - 22

Opposizione al trattamento ed alla profilazione.

Sezione 5 - limitazioni art. 23

Esistono limitazioni all'esercizio dei diritti

Capo IV - Titolare e responsabile del trattamento

Si individuano i soggetti che effettuano i trattamenti

Sezione 1 - obbligh generali art. 24 - 31

Sono articoli con principi importanti, si individuano le responsabilità, ed il principo di protezione "by default and by design", si individua la figura del Responsabile del trattamento e si dichiara che gli addetti hanno un obbligo di riservatezza. Viene anche introdotto l'obbligo formale della tenuta delo "Registro delle attività di trattamento"

Sezione 2 - Sicurezza dei dati personali art. 32 - 34

Si esorta il titolare a mettere in atto le misure tecniche atte a garantire la sicurezza. Le misure dovranno essere adeguate ma proporzionali alla natura del trattamento, non si entra nel merito delle soluzione tecniche, ma si fissano gli obiettivi. Si indicano anche le regole da adottare in caso di violazione dei dati.

Sezione 3 - Valutazione di impatto e consultazione preventiva art. 35 - 36

Prima di attuare il trattamento si deve valutare l'impatto del trattamento ed in caso di dubbio consultare preventivamente l'autorità di controllo.

Sezione 4 - Responsabile della protezione dei dati art. 37 - 39

La nuova figura del Responsabile della protezione dei dati è un esperto della normativa che vigila sulla sua applicazione e fa da raccordo tra il titolare e l'autorità di controllo.

Sezione 5 - Codici di condotta e certificazione art. 40 - 43

I codici di condotta sono organizzati per categorie di titolari e servono a delineare fattori comuni tra i soggetti. L'autorità di controllo riconosce i codici di condotta approvati per categoria e ne controlla la conformità rispetto al regolamento. Consegue la possibilità del rilascio di certificazioni utili a valutare la conformità del trattamento.

Capo V - Trasferimento di dati verso Paesi Terzi

Art. da 44 a 50

Il trasferimento di dati personali presso Paesi Terzi può avvenire solo se vengono rispettati i requisiti di sicurezza richiesti dalla UE, la Commissione individua i reguisiti dei vari Paesi, in assenza di tale valutazione esistono requisiti che il titolare deve considerare per effettuare il trasferimento.

Capo VI - Autorità di controllo indipendenti

Sezione 1 - Indipendenza art. 51 - 54

Gli stati membri dispongono di autorità di controllo che agisce in piena indipendenza. Ogni Stato membro istitusce regole per la nomina delle autorità di controllo.

Sezione 2 - competenze, compiti e poteri 55 -59

L'autorità di controllo è competente per l'applicazione del regolamento ed ha alcuni compiti di controllo e promozione, nonché poteri per vigilare sulla applicazione del regolamento.

Capo VII - Cooperazione e coerenza

Sezione 1 - cooperazione art. 60 - 62

Vengono stabilite regole per la cooperazione tra le diverse autorità di controllo

Sezione 2 - Coerenza art. 63 - 67

La coerenza riguarda l'applicazione uniforme del regolamento nei paesi della UE

Sezione 3 - Comitato europeo per la protezione dei dati art. 68 - 76

Viene istituito un comitato europeo con una propria struttura organizzativa

Capo VIII - Mezzi di ricorso, responsabilità e sanzioni

Art. da 77 a 84

Vengono specificati modi e forme che gli interessati hanno per opporre reclamo. Vengono stabilite sanzioni che possono raggiungere i 4% del fatturato mondiale della impresa che ha commesso una violazione.

Capo IX - Disposizioni relative a specifiche situazioni del trattamento

Art. da 85 a 91

Esistono campi specifici in cui ci possono essere deroghe ai principi ed ai diritti degli interessati. Ad esempio per tutelare la libertà di informazione, l'accesso a documenti pubblici, i rapporti di lavoro ed il pubblico interesse.

Capo X - Atti delegati e atti di esecuzione

Art. da 92 a 93

Su alcune materie la Commissione ha il potere di delegare terzi. Viene anche istituito un comitato con il compito di assistere la Commissione

Capo XI - Disposizioni finali

Si stabiliscono le relazioni con norme precedenti o relazionate. Si stabiliscono regole per l'adeguamento nel tempo e si stebilisce che la norma entra in vigore dal 25 maggio 2018.