Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo"
Consiglio Nazionale delle Ricerche

ISTI Technical Reports

Un modello di designazione dell'amministratore di sistema realizzato per il Consiglio Nazionale delle Ricerche in applicazione del Regolamento (UE) 2016/679 sulla protezione dei dati personali

Valentina Amenta, CNR-IIT, Pisa, Italy

Rosaria Deluca, CNR-ISTI, Pisa, Italy

Andreina Fullone, CNR-Dipartimento di Scienze Biomediche, Rome, Italy

Alessia Glielmi, CNR-Direzione Generale, Rome, Italy

Massimo Ippoliti, CNR-Direzione Generale, Rome, Italy

Olga Micolitti, CNR-Direzione Generale, Rome, Italy

Daniela Niccoli, CNR-Centro Interdipartimentale per l'etica e l'integrità nella ricerca, Rome, Italy

ISTI-TR-2022/019

Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo"
Consiglio Nazionale delle Ricerche

Un modello di designazione dell'amministratore di sistema realizzato per il Consiglio Nazionale delle Ricerche in applicazione del Regolamento (UE) 2016/679 sulla protezione dei dati personali

Amenta V.; Deluca R.; Fullone A.; Glielmi A.; Ippoliti M.; Micolitti O.; Niccoli D.

ISTI-TR-2022/019

Abstract

Predisposizione di un modello esemplificativo per la designazione della figura di amministratore di sistema, modulabile sulle base delle effettive specificità delle strutture CNR.

Privacy, Security

Citation

Amenta V.; Deluca R.; Fullone A.; Glielmi A.; Ippoliti M.; Micolitti O.; Niccoli D. *Un modello di designazione dell'amministratore di sistema realizzato per il Consiglio Nazionale delle Ricerche in applicazione del Regolamento (UE) 2016/679 sulla protezione dei dati personali* ISTI Technical Reports 2022/019. DOI: 10.32079/ISTI-TR-2022/019

Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo"
Area della Ricerca CNR di Pisa
Via G. Moruzzi 1
56124 Pisa Italy
http://www.isti.cnr.it

RAPPORTO TECNICO

UN MODELLO DI DESIGNAZIONE DELL'AMMINISTRATORE DI SISTEMA REALIZZATO PER IL CONSIGLIO NAZIONALE DELLE RICERCHE IN APPLICAZIONE DEL REGOLAMENTO UE 2016/679 SULLA PROTEZIONE DEI DATI PERSONALI

INTRODUZIONE

Autori CNR: Valentina Amenta, (Istituto di Informatica e Telematica), Rosaria Deluca, (Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo"), Andreina Fullone (Dipartimento Scienze Biomediche), Alessia Glielmi (Ufficio Servizi Generali-Direzione Generale), Massimo Ippoliti (Unità supporto agli organi–Direzione Generale), Olga Micolitti (Ufficio ICT-Direzione Generale), Daniela Niccoli (Associato Senior Centro Interdipartimentale per l'etica e l'integrità nella ricerca).

Con il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 ("Regolamento") relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione in vigore dal 24 maggio 2016, applicabile a partire dal 25 maggio 2018, è sorta la necessità di dare piena e corretta applicazione alle nuove disposizioni. Il successivo Decreto legislativo 10 agosto 2018, n. 101 ("Decreto di Adeguamento") ha reso coerente il Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali ("Codice privacy") alle disposizioni del Regolamento.
Ravvisata analoga necessità anche il C.N.R. ha provveduto ad aggiornare il nuovo assetto organizzativo dell'Ente nel contesto relativo alla protezione dei dati personali in coerenza con il Regolamento e con il Codice Privacy mediante il ricorso all'art. 2-quaterdecies, Codice Privacy rubricato "Attribuzione di funzioni e compiti a soggetti designati". Quest'ultimo, infatti, così recita "*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*".
Il nuovo assetto organizzativo è ora delineato nel vigente Regolamento di Organizzazione e Funzionamento (R.O.F.) del Consiglio Nazionale delle Ricerche (C.N.R.), emanato con provvedimento del Presidente n. 14 di cui al protocollo AMMCNT – CNR n. 12030 del 18 febbraio 2019 di cui è stato dato l'avviso di pubblicazione sul sito del Ministero dell'Istruzione, dell'Università e della Ricerca il 19 febbraio 2019, che è entrato in vigore il 1°marzo 2019.
Sul punto corre evidenziare come: mentre l'art 19-bis (Protezione dei dati personali) comma 1 del R.O.F. del C.N.R. ha introdotto, ai fini dell'applicazione delle norme sulla protezione dei dati personali, le definizioni delle figure coinvolte, il successivo comma 4, prevede l'attribuzione dei compiti e delle funzioni ai corrispondenti del responsabile della protezione dei dati e *all'introduzione di ulteriori misure organizzative tali da assicurare una distribuzione di compiti coerente con gli assetti organizzativi dell'ente* e di adeguate strutture di supporto al Direttore generale e al responsabile della protezione dei dati.
Il successivo Provvedimento del Presidente n. 27 Prot. AMMCNT-CNR n. 0064997/2019 del 20.09.2019, così come previsto dall'art. 19-bis, comma 4, ha definito i compiti e le funzioni dei responsabili interni, punto di contatto del titolare, punto 1 lettera n) nel Provvedimento in argomento che cosi decreta: "*vigilano sull'osservanza da parte dei soggetti autorizzati al trattamento che operano sotto la loro diretta autorità delle normative in materia di protezione dei dati personali e delle misure tecniche e organizzative adottate per la protezione dei dati dalle strutture di competenza*".
Sul punto corre richiamare l'art 29 del Regolamento rubricato "Trattamento sotto l'autorità del titolare o del responsabile del trattamento" prescrive che "*Il titolare del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del responsabile del trattamento, che abbia accesso ai dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli stati membri*".
L'art. 29 introduce un adempimento di carattere generale rilevante alla protezione dei dati personali.

L'individuazione e la formazione dei soggetti che agiscono sotto l'autorità del titolare o del responsabile del trattamento cosi come la loro formazione nella previsione che gli stessi possano trattare i dati personali solo se opportunamente istruiti è strettamente connessa ai principi fondamentali di cui all'art. 5 del Regolamento.
In relazione alla figura dell'incaricato del trattamento, occorre evidenziare che mentre nell'art. 30 del Codice Privacy, abrogato dal Decreto di adeguamento questa figura era espressamente prevista, analoga figura non è riscontrabile né nel Regolamento né nel Codice privacy così come novellato dal Decreto di adeguamento. L'attualità di tale figura può essere ricavata dalle ricostruzioni operate dall'Autorità garante e delle vigenti normative.
Tra i soggetti autorizzati al trattamento ex art. 29 è presente l'amministratore di sistema, - figura che non viene espressamente richiamata né nel Regolamento né direttamente nella versione precedente del Codice privacy - ma solo indirettamente mediate le funzioni tipiche dell'amministratore di sistema contenute nell'all. b al Codice privacy. La definizione dell'amministratore di sistema deve essere ricavata dunque nell'art. 1, comma 1, lett. c) DPR n. 318/1999 che così recitava: "*soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione*". Oggi la definizione è presente nel provvedimento dell'Autorità Garante avente ad oggetto "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008" pubblicato su G.U. n. 300 del 24 dicembre 2008 e successivamente modificato in base al provvedimento del 25 giugno 2009 pubblicato su G.U. n. 149 del 30 giugno 2009 ("Provvedimento") reperibile al link https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1577499 e più in particolare all'art. 1 comma 1 secondo il quale "*con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente provvedimento vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi*". Per sua natura l'amministratore di sistema è figura cui sono richieste competenze specifiche, infatti il provvedimento in argomento all'art. 4.1 rubricato "*Valutazione delle caratteristiche soggettive*" così recita: "*l'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell´esperienza, della capacità e dell´affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza*".
La nomina dell'amministratore di sistema deve intendersi collocata nell'ambito più ampio del principio di accountability (responsabilizzazione) che è presente trasversalmente nel Regolamento e più in particolare tra le misure tecniche-organizzative per le quali, in tale ambito, è prevista sia a norma del Regolamento che a norma dell'art. 4.4 rubricato "*Verifica delle attività*" del richiamato provvedimento del 2008. Essa così recita: "*L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari o dei responsabili del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti*".
La designazione dell'amministratore di sistema rientra a tutti gli effetti tra le misure tecniche-organizzative e anche alla luce della cadenza, almeno annuale, della verifica relativa alle attività svolte da effettuarsi a cura del titolare oppure del responsabile, deve essere oggetto di riesame e aggiornamento qualora necessario.
La designazione ad amministratore di sistema deve essere individuale e contenere l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. A norma del provvedimento dell'Autorità Garante sopra richiamato il titolare deve disporre di un elenco recante i nominativi degli amministratori e delle relative funzioni ad essi attribuite.
Il titolare a norma dell'art. 4 comma 1 del Provvedimento è tenuto ad assicurare che "*gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, siano annotati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante*".
In un'ottica di trasparenza del trattamento il titolare a norma dell'art. 4 comma 2 del Provvedimento così recita: "*Qualora l´attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori, i titolari*

pubblici e privati nella qualità di datori di lavoro sono tenuti a rendere nota o conoscibile l´identità degli amministratori di sistema nell´ambito delle proprie organizzazioni, secondo le caratteristiche dell´azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell´informativa resa agli interessati ai sensi dell´art. 13 del Codice nell´ambito del rapporto di lavoro che li lega al titolare, oppure tramite il disciplinare tecnico la cui adozione è prevista dal provvedimento del Garante n. 13 del 1° marzo 2007 (in G.U. 10 marzo 2007, n. 58); in alternativa si possono anche utilizzare strumenti di comunicazione interna (a es., intranet aziendale, ordini di servizio a circolazione interna o bollettini). Ciò, salvi i casi in cui tale forma di pubblicità o di conoscibilità non sia esclusa in forza di un´eventuale disposizione di legge che disciplini in modo difforme uno specifico settore.

La designazione dell'amministratore di sistema può riguardare sia un soggetto interno che un soggetto esterno. In questo secondo caso, il titolare, ricorrendone la necessità, può nominare un Responsabile ex art. 28 GDPR purché in possesso dei requisiti previsti dal paragrafo 1, e cioè a dire nel caso di trattamenti da effettuarsi per suo conto 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* in omaggio, anche nel caso di specie al principio di accountability.

Quando il ruolo di amministratore di sistema viene affidato in outsourcing ad un soggetto esterno, questo dovrà considerarsi altresì un responsabile del trattamento. In virtù di ciò, il titolare dovrà vincolare l'amministratore di sistema con un contratto scritto, contenente tutti i requisiti richiesti dall'art. 28 Reg. UE 2016/679. Ogni volta in cui un titolare del trattamento decida di affidare in outsourcing la manutenzione dei propri sistemi informatici, deve assicurarsi che il soggetto incaricato sia dotato di comprovate capacità tecniche, esperienza e affidabilità, tali da garantire il pieno rispetto della normativa in materia di protezione dei dati personali, compreso il profilo della sicurezza.

La nomina di un responsabile, infatti, non esime il titolare dall'eventuale *culpa in eligendo* e cioè nel caso di nomina di un responsabile non in possesso di garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate nonché della "*culpa in vigilando*" dovuta al mancato controllo delle attività delegate al responsabile.

La forma scritta *ad substantiam*, anche elettronica, richiesta dall'art. 28 GDPR rappresenta infatti solo una cornice del contratto o dell'atto giuridico a norma del diritto dello Stato o dell'Unione che disciplinerà e definirà in dettaglio gli elementi richiesti a norma del paragrafo 3 non essendo consentito al titolare delegare il controllo nei confronti del responsabile.

La Commissione con la decisione in nota[1] ha recentemente approvato le clausole contrattuali tipo che soddisfano i requisiti per i contratti tra titolari del trattamento e responsabili del trattamento di cui all'articolo 28, paragrafi 3 e 4, del regolamento (UE) 2016/679 e all'articolo 29, paragrafi 3 e 4, del regolamento (UE) 2018/1725.

Al titolare è richiesto un ruolo proattivo per documentare quanto previsto nell'art. 28, par. 1 del GDPR e quindi dover dimostrare l'accountability. Esso può essere esonerato da rivendicazioni di terzi per azioni cagionate non conformi ai dettati degli accordi con il responsabile esclusivamente nel caso in cui il responsabile fatti salvi gli arti. 82, 83, e 84 del GDPR violi il GDPR determinando finalità e mezzi del trattamento è considerato titolare del trattamento in argomento.

Nel caso di servizi di amministrazione di sistema affidati in *outsourcing*, mediante la nomina di un responsabile ex art. 28, il titolare o il responsabile del trattamento devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

La ricostruzione circa l'attualità della figura dell'incaricato operata dall'Autorità garante è disponibile nella "Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali" e presente alla seguente pagina web: https://www.garanteprivacy.it/regolamentoue/titolare-responsabile-incaricato-del-trattamento.

Nel contesto normativo, occorre prendere avvio dalla definizione di "terzo" contenuta nel Regolamento *(si veda, in particolare, art. 4, n. 10, del regolamento)* e che viene qualificato come "la

[1] Decisione di esecuzione (UE) 2021/915 della Commissione del 4 giugno 2021 relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio e dell'articolo 29, paragrafo 7, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio (Testo rilevante ai fini del SEE). https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32021D0915&from=EN.

persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato. Il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile". Non quindi una definizione diretta ma una definita quindi a contrario.
L'intento è sostanzialmente duplice da un lato si prefigge di agevolare l'individuazione di una prima base di misure tecniche e organizzative incentivando il raggiungimento di un livello adeguato delle misure stesse dall'altro si prefigge di raggiungere una modalità, per quanto possibile omogenea di tali misure tra le strutture del C.N.R. pur nel rispetto dell'esigenza, di salvaguardare le peculiarità e necessità di ciascuna struttura.
L'adozione, il monitoraggio e qualora necessario l'aggiornamento delle misure adeguate dovrà ovviamente avvenire a cura e sotto l'esclusiva responsabilità del titolare e quindi nel caso di specie del responsabile interno.
La pluralità ed eterogeneità delle strutture, sia dell'Amministrazione Centrale che della Rete scientifica è certamente una ricchezza per l'Ente ed implica al tempo stesso l'impossibilità di rendere completamente omogenee le misure tecniche-organizzative, sostanziandosi un tale approccio in contrasto con il principio di accountability. Ciò nonostante, e seppur in forma parziale, alcune misure tecniche-organizzative da adottare sono adottabili su una base comune almeno per i trattamenti omogenei e che sono ricorrenti in tutte le strutture dell'ente.
Si evidenzia infine come la mancata adozione delle misure previste dall'art 29 del Regolamento espone il C.N.R. ad un duplice rischio: a) la sanzione amministrativa che può raggiungere l'importo di 10.000.000 di euro, art. 83, par. 4 lettera a) del Regolamento; b) il risarcimento degli eventuali danni derivanti dalla violazione del Regolamento così come previsto dall'art. 82 paragrafo 1 dello stesso.

Nomina dell'amministratore di sistema ai sensi e per gli effetti del Regolamento UE 2016/679 sulla protezione dei dati personali (nel seguito "GDPR") per [Nome Struttura]

Oggetto: nomina di ____ quale amministratore di sistema.

Premesso che:

VISTO il Decreto Legislativo 4 giugno 2003 n.127 recante disposizioni per il riordino del Consiglio Nazionale delle Ricerche;
VISTO il Decreto legislativo 31 dicembre 2009, n. 213 "Riordino degli Enti di ricerca in attuazione dell'art.1 della legge 27 settembre 2007, n.165";
VISTO il Decreto Legislativo 25 novembre 2016, n.218 "Semplificazione delle attività degli Enti pubblici di ricerca ai sensi dell'art. 13 della legge 7 agosto 2015, n.124";
VISTO il Decreto Legislativo 30 giugno 2003, n.196 "Codice in materia di protezione dei dati personali";
VISTO il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla Protezione dei dati"), in vigore dal 24 maggio 2016 e applicabile a partire dal 25 maggio 2018;
VISTO il Regolamento di organizzazione e funzionamento del Consiglio Nazionale delle Ricerche, emanato con provvedimento del Presidente n. 14 di cui al protocollo AMMCNT – CNR n. 12030 del 18 febbraio 2019 di cui è stato dato l'avviso di pubblicazione sul sito del Ministero dell'Istruzione, dell'Università e della Ricerca il 19 febbraio 2019, entrato in vigore il 1°marzo 2019;
VISTA la Circolare CNR Regolamento generale sulla protezione dei dati UE 2016/679 "Registro delle attività di trattamento dei dati". Modalità procedurali per l'aggiornamento e il caricamento informatico (Prot n. 0084613/2019 del 27/11/2019);
VISTO il comma 4 dell'art. 19 bis (Protezione dei dati personali) del Regolamento di organizzazione e funzionamento, che prevede l'attribuzione dei compiti e delle funzioni ai corrispondenti del Responsabile della Protezione dei Dati e all'introduzione di ulteriori misure organizzative tali da assicurare una distribuzione di compiti coerente con gli assetti organizzativi dell'Ente e di adeguate strutture di supporto al Direttore generale e al Responsabile della Protezione dei Dati;
VISTI l'art. 29 del GDPR "Trattamento sotto l'autorità del Titolare del trattamento o del Responsabile del trattamento" e l'art 32 del GDPR "Sicurezza del trattamento";

VISTO il D.P.R. 16 aprile 2013, n. 62, Regolamento recante il codice di comportamento dei dipendenti pubblici, a norma dell'art. 54 del decreto legislativo 30 marzo 2001, n. 165;
VISTO il Codice di comportamento del CNR – Aggiornamento - Il Consiglio di Amministrazione nella riunione del 17 ottobre 2017, ha adottato all'unanimità dei presenti la seguente deliberazione n. 137/2017 – Verb. 335;
CONSIDERATO che AFLEG deve procedere all'adeguamento dell'organizzazione interna come previsto dal Provvedimento del Presidente n. 27/2019;
VISTO il provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, G.U. n. 300 del 24 dicembre 2008 (Misure e accorgimenti prescritti a titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema) come modificato dal provvedimento del Garante per la protezione dei dati personali del 25 giugno 2008, G.U. n. 300 del 25 giugno 2009;
……

Dispone

Classificare analiticamente le banche dati ed impostare/organizzare un sistema complessivo di trattamento dei dati personali sia identificativi che particolari e giudiziari (art. 9 e 10 GDPR predisponendo ogni relativa fase applicativa e nel rispetto della normativa vigente in materia di protezione dei dati personali;
Individuare il soggetto incaricato della custodia delle parole chiave per l'accesso al sistema informativo e vigilare sulla sua attività;
Individuare per iscritto gli altri soggetti diversi dall'incaricato della custodia delle parole chiave che possono avere accesso alle informazioni che concernono le medesime;
Impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici, conforme a quanto previsto dall'art 32 GDPR;
Impostare e gestire un sistema di autorizzazione per gli incaricati dei trattamenti di dati personali con strumenti elettronici;
Adottare un sistema idoneo alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici; le registrazioni (access log) devono avere caratteristica di completezza, inalterabilità e possibilità di verifica della loro integrità adeguata al raggiungimento dello scopo di verifica per cui sono richieste; tali registrazioni devono comprendere i riferimenti temorali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;
Assicurare e gestire sistemi di salvataggio e di ripristino dei dati (backup/recovery), anche automatici nonché approntare adeguate misure e/o sistemi software di salvaguardia per la protezione dei dati personali (antivirus, firewall, IDS) sempre nel rispetto dell'art 32 GDPR;
Impartire a tutti gli autorizzati istruzioni organizzative e tecniche che prevedano le modalità di utilizzo dei sistemi di salvataggio dei dati con frequenza almeno settimanale;
Adottare procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi;
Organizzare i flussi di rete, la gestione dei supporti di memorizzazione, la manutenzione hardware, la verifica delle le condotte di accesso e/o la permanenza nei sistemi informatici dell'Ente per ragioni estranee e comunque diverse rispetto a quelle per le quali sono stati abilitati costituisce che integrano il reato di accesso abusivo ai sistemi informatici e telematici (art 615-*ter* c.p.), le condotte che integrano il reato di "Detenzione e diffusione abusive dei codici di accesso a sistemi informatici o telematici (art 615-*quater* c.p.) nonché le condotte che integrano il reato di "Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico telematici (art 615-*quinques* c.p.).
Sara oggetto di verifica inoltre le condotte di "Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità" (art 635-*ter* c.p.) nonché le condotte di "Danneggiamento di sistemi informatici o telematici di pubblica utilità" (art 635-*quinquies* c.p.), le condotte che integrano il delitto di frode informatica (art. 392, comma 3 c.p.) ed inoltre la condotta di esercizio arbitrario delle proprie ragioni con violenza sulle cose (art. 392, comma 3 c.p.).
Predisporre, anche in contraddittorio con il titolare dei trattamenti, un piano di controlli periodici, da eseguirsi con cadenza almeno semestrale, atti a verificare l'efficacia delle misure di sicurezza adottate;
E' compito dell'amministratore di sistema monitorare costantemente lo stato di sicurezza di tutti i processo di elaborazione dati di cui sopra, mantenendo aggiornati tutti i supporti hardware e software e, se del caso, comunicando al titolare tutte le attività da porre in essere al fine di garantire un adeguato livello di sicurezza in proporzione alla tipologia e qualità dei dati personali trattati.

L'operato dell'amministratore di sistema sarà oggetto, con cadenza annuale, ad una attività di verifica da parte del titolare del trattamento, tesa aa controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto al trattamento dei dati personali previsti dalle norme vigenti.
……..

Principali fonti normative, provvedimenti dell'Autorità Garante e informative interne

1) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 aggiornato alle rettifiche pubblicate sulla Gazzetta Ufficiale dell'Unione europea 127 del 23 maggio 2018;

2) DECRETO LEGISLATIVO 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali" ss.mm.ii.;

*3) P*rovvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, G.U. n. 300 del 24 dicembre 2008 (Misure e accorgimenti prescritti a titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema) come modificato dal provvedimento del Garante per la protezione dei dati personali del 25 giugno 2008, G.U. n. 300 del 25 giugno 2009;

4) Lavoro: le linee guida del Garante per posta elettronica e internet;

5) Notifica delle violazioni dei dati personali;

6) Provvedimento del Garante notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019. Il modello elettronico è ora reperibile al seguente indirizzo: https://www.garanteprivacy.it/regolamentoue/databreach;

7) Modello data breach;

8) GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI Versione emendata e adottata in data 6 febbraio 2018 - 18/IT WP250 rev.01. Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679;

9) Linee guida cookie e altri strumenti di tracciamento - 10 giugno 2021;

10) Deliberazione del 4 aprile 2019 - Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali *(Pubblicato sulla Gazzetta Ufficiale n. 106 dell'8 maggio 2019);*

11) Indicazioni al personale in materia di sicurezza informatica;

12) I suggerimenti del Garante per proteggersi dal phishing.