GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

PROVVEDIMENTO 2 luglio 2015

Misure di sicurezza e modalita' di scambio dei dati personali tra amministrazioni pubbliche. (Provvedimento n. 393). (15A05952)

(GU n.179 del 4-8-2015)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

Visto il decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali (di seguito Codice);

Visto il decreto legislativo 7 marzo 2005, n. 82, Codice dell'amministrazione digitale (di seguito Cad);

Considerate le peculiari caratteristiche delle banche dati delle amministrazioni pubbliche, contraddistinte, in particolare, dall'ingente mole di dati trattati, dalla delicatezza delle informazioni ivi contenute e dalla molteplicita' di soggetti autorizzati ad accedervi, nonche' l'esigenza di garantire costantemente l'esattezza, l'integrita' e la disponibilita' dei dati personali ivi contenuti non solo in relazione alle c. d. basi dati di interesse nazionale (art. 60 del Cad), unitamente agli specifici rischi di accesso non autorizzato e di trattamento non consentito;

Ritenuto necessario assoggettare il trattamento dei dati personali effettuato nell'ambito delle predette banche dati all'obbligo di comunicazione al Garante del verificarsi di violazioni dei dati o incidenti informatici (accessi abusivi, azione di malware) che, pur non avendo un impatto diretto su di essi, possano comunque esporli a rischi di violazione;

Ritenuto, pertanto, che le pubbliche amministrazioni di cui all'art. 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165 debbano comunicare al Garante, entro quarantotto ore dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati (c.d. data breach) e che tali comunicazioni devono essere redatte secondo lo schema riportato nell'Allegato 1 al presente provvedimento e inviate tramite posta elettronica o posta elettronica certificata all'indirizzo: databreach.pa@pec.gpdp.it;

Vista, inoltre, la nuova formulazione dell'art. 58, comma 2, del Cad, cosi' come modificato dall'art. 24-quinquies, comma 1, decreto-legge 24 giugno 2014, n. 90, convertito, con modificazioni, dalla legge 11 agosto 2014, n. 114, in vigore dal 19 agosto 2014, la quale ha previsto che «le pubbliche amministrazioni comunicano tra

loro attraverso la messa a disposizione a titolo gratuito degli accessi alle proprie basi di dati alle altre amministrazioni mediante la cooperazione applicativa di cui all'art. 72, comma 1, lettera e). L'Agenzia per l'Italia digitale, sentiti il Garante per la protezione dei dati personali e le amministrazioni interessate alla comunicazione telematica, definisce entro novanta giorni gli standard di comunicazione e le regole tecniche a cui le pubbliche amministrazioni devono conformarsi»;

Considerato che tale modifica ha superato, quindi, il pregresso impianto normativo relativo all'accessibilita' telematica ai dati delle pubbliche amministrazioni, fondato su «apposite convenzioni aperte all'adesione di tutte le amministrazioni interessate volte a disciplinare le modalita' di accesso ai dati da parte delle stesse amministrazioni procedenti» (testo previgente dell'art. 58, comma 2 del Cad);

Considerato, altresi', che il Garante, nell'ambito del parere del 4 luglio 2013 (doc. web n. 2574977) sulle apposite linee guida dell'Agenzia per l'Italia digitale (di seguito Agid) per la stipula delle predette convenzioni aperte aveva prescritto alle amministrazioni destinatarie delle stesse l'adozione di specifiche misure tecniche e organizzative;

Considerato che nel trattamento di dati personali l'erogatore (amministrazione titolare del trattamento dei dati personali che mette a disposizione i relativi servizi di accesso) e il fruitore (amministrazione richiedente che accede in qualita' di autonomo titolare ai dati personali resi disponibili dall'erogatore) sono chiamati a rispettare il Codice con particolare riferimento ai presupposti che legittimano i flussi di dati e agli adempimenti in materia di misure di sicurezza;

Ritenuto necessario, pertanto, nelle more della definizione da parte dell'Agid dei suindicati «standard di comunicazione e le regole tecniche», confermare le specifiche misure tecniche e organizzative gia' individuate, prescrivendo nuovamente l'adozione delle stesse - riportate nell'Allegato 2 al presente provvedimento - al fine di ridurre al minimo i rischi di accessi non autorizzati o di trattamenti non consentiti o non conformi alle finalita' della raccolta dei dati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento ai sensi dell'art. 31 del Codice, salvo che le modalita' di accesso alle banche dati siano gia' state oggetto di esame da parte del Garante nell'ambito di specifici provvedimenti;

Rilevato che le misure necessarie individuate nell'Allegato 2, adeguate al nuovo contenuto del citato art. 58, comma 2, nella sostanza risultano equivalenti a quelle prescritte dal Garante nell'ambito del predetto parere sulle linee guida dell'Agid del 4 luglio 2013;

Ritenuto, pertanto, che le convenzioni gia' predisposte dalle amministrazioni nel rispetto del richiamato parere del Garante, anche al fine di garantire il rispetto del principio di semplificazione, debbano ritenersi conformi alle misure necessarie individuate nell'Allegato 2 al presente provvedimento;

Ritenuto, invece, che laddove siano state previste modalita' di accesso ai dati personali ai sensi della nuova formulazione del predetto art. 58, comma 2 del Cad, non conformi alle misure gia' individuate dal Garante nel citato provvedimento del 4 luglio 2013, le misure previste nell'Allegato 2 debbano essere adottate dalle amministrazioni interessate entro e non oltre il 31 dicembre 2015;

Rilevato, infine, che la mancata comunicazione al Garante dei c.d. data breach, nonche' la mancata adozione delle misure necessarie individuate nell'Allegato 2 al presente provvedimento nei suesposti termini e modalita', configurano un illecito amministrativo sanzionato ai sensi dell'art. 162, comma 2-ter del Codice;

Vista la documentazioni in atti;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;
Relatore la dott.ssa Augusta Iannini;

Tutto cio' premesso il Garante:

1. Ai sensi dell'art. 154, comma 1, lett. c), del Codice, prescrive che le pubbliche amministrazioni di cui all'art. 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165 devono comunicare al Garante, entro quarantotto ore dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati e che tali comunicazioni debbano essere redatte secondo lo schema riportato nell'Allegato 1 al presente provvedimento e inviate tramite posta elettronica o posta elettronica certificata all'indirizzo: databreach.pa@pec.gpdp.it;
2. Ai sensi dell'art. 154, comma 1, lett. c), del Codice, nelle more della definizione degli «standard di comunicazione e le regole tecniche» da parte dell'Agid ai sensi dell'art. 58, comma 2, del Cad, prescrive alle pubbliche amministrazioni che intendano mettere a disposizione gli accessi alle proprie banche dati alle altre amministrazioni che ne abbiano diritto mediante la cooperazione applicativa di cui all'art. 72, comma 1, lettera e) del Cad l'adozione delle misure necessarie individuate nell'Allegato 2 al presente provvedimento, salvo che le modalita' di accesso alle banche dati siano gia' state oggetto di esame da parte del Garante nell'ambito di specifici provvedimenti; laddove siano gia' state previste modalita' di accesso ai sensi della nuova formulazione del predetto art. 58, comma 2 del Cad, non conformi alle misure gia' individuate dal Garante nel provvedimento del 4 luglio 2013, prescrive che le misure necessarie previste nell'Allegato 2 siano adottate dalle amministrazioni interessate entro e non oltre il 31 dicembre 2015;
3. Ai sensi dell'art. 143, comma 2, del Codice dispone la trasmissione di copia del presente provvedimento al Ministero della giustizia - Ufficio pubblicazione leggi e decreti, per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 2 luglio 2015

Il presidente: Soro

Il relatore: Iannini

Il segretario generale: Busia

Allegato 1

Parte di provvedimento in formato grafico

Allegato 2

Misure necessarie

1. Modalita' d'accesso.

Le pubbliche amministrazioni che intendono rendere fruibili diverse tipologie di dati da altre pubbliche amministrazioni, tenuto conto degli obiettivi di carattere generale perseguiti dal Cad e dell'attuale quadro infrastrutturale disponibile sul territorio, utilizzano le seguenti opzioni tecniche:

accesso via web, attraverso il sito istituzionale dell'erogatore, un sito tematico appositamente predisposto o altre applicazioni

software;

accesso in modalita' di cooperazione applicativa, componente del sistema pubblico di connettivita' finalizzata all'interazione tra i sistemi informatici delle pubbliche amministrazioni per garantire l'integrazione dei metadati, delle informazioni e dei procedimenti amministrativi.

Ferme restando le modalita' di accesso telematico definite al punto precedente, che devono considerarsi quelle di riferimento ai fini dell'attuazione delle norme in materia di fruibilita' dei dati, le amministrazioni possono utilizzare modalita' alternative, laddove si presentino documentabili vantaggi economici o la situazione infrastrutturale e organizzativa non consenta l'adozione di quelle sopra riportate. Le predette circostanze devono essere adeguatamente documentate. In tali casi, le modalita' di accesso telematico prevedibili sono:

la posta elettronica certificata, nei casi specifici, quando la periodicita' di acquisizione del dato e' limitata (in linea di massima una volta all'anno o meno) e la quantita' dei dati da acquisire e' contenuta;

soluzioni di "Trasferimento di File" in modalita' FTP "sicuro" o equivalente dal punto di vista della sicurezza del trasporto, qualora preesistenti investimenti, la natura stessa delle richieste e le specifiche condizioni facciano propendere per tale soluzione garantendo la cifratura del canale di trasmissione dei dati (ad esempio, utilizzando meccanismi quali le reti private virtuali o la cifratura delle sessioni di trasferimento dei dati).

2. Presupposti per la comunicazione di dati personali.

La convenzione (ovvero qualsivoglia atto bilaterale stipulato tra erogatore e fruitore al fine di stabilire le condizioni e le modalita' di accesso ai dati) e' lo strumento in cui le amministrazioni possono stabilire le garanzie - anche nei confronti dello stesso erogatore - a tutela del trattamento dei dati personali e dell'utilizzo dei sistemi informativi.

Di seguito vengono pertanto individuati misure e accorgimenti da attuare al fine di assicurare la correttezza del trattamento e di ridurre rischi nell'utilizzo dei dati personali.

In ogni caso l'erogatore, al fine di salvaguardare la sicurezza dei propri sistemi informativi, anche in considerazione delle caratteristiche delle banche dati accessibili attraverso la convenzione, e' tenuto a valutare l'introduzione di ulteriori strumenti volti a gestire i profili di autorizzazione, verificare accessi anomali, tracciare le operazioni di accesso, ovvero individuare tassative modalita' di accesso alle banche dati, dandone conto nella convenzione (art. 31 del Codice).

2.1 Verifiche preliminari a cura dell'erogatore.

L'erogatore prima di stipulare ogni singola convenzione per l'accesso alle proprie banche dati in via telematica deve verificare:

a) la base normativa che legittima il fruitore ad accedere alle proprie banche dati (per i dati diversi da quelli di sensibili e giudiziali: norma di legge o di regolamento, ovvero previa comunicazione al Garante ai sensi dell'art. 19, comma 2 del Codice, qualora manchi una norma di legge o di regolamento e il flusso di dati risulti necessario per lo svolgimento delle proprie funzioni istituzionali; per i dati sensibili e giudiziari: la norma di legge che autorizzi il trattamento e l'individuazione nella stessa, o in atto di natura regolamentare adottato in conformita' al parere del Garante, dei tipi di dati e le operazioni eseguibili);

b) la finalita' istituzionale perseguita dal fruitore (ad esempio controllo sulle dichiarazioni sostitutive) e la natura e la qualita' dei dati richiesti, selezionando accuratamente le informazioni personali contenute nelle banche dati a cui dare accesso;

c) la modalita' telematica di accesso alle banche dati piu' idonea rispetto alle finalita', alla natura e alla quantita' dei dati, alle caratteristiche anche infrastrutturali e organizzative del

fruitore, al volume e alla frequenza dei trasferimenti, al numero di soggetti abilitati all'accesso.

2.2 Selezione dei dati.

La selezione delle informazioni personali oggetto di accesso deve avvenire nel rispetto dei principi di pertinenza e non eccedenza in relazione a ciascuna delle finalita' perseguite dal fruitore. Rispetto ad una medesima banca dati devono essere, infatti, prefigurati diversi livelli e modalita' di accesso che offrano al fruitore unicamente i dati necessari per le proprie esigenze istituzionali.

Le modalita' di accesso alle banche dati devono essere, pertanto, configurate offrendo un livello minimo di accesso ai dati, anche limitando i risultati delle interrogazioni a valori di tipo booleano (ad es., web services che forniscono un risultato di tipo vero/falso nel caso di controlli sull'esistenza o sulla correttezza di un dato oggetto di autocertificazione). Livelli di accesso gradualmente piu' ampi possono essere autorizzati soltanto a fronte di documentate esigenze del fruitore da indicare in convenzione.

E' chiaro, inoltre, che per ciascun fruitore possono essere individuate piu' modalita' di accesso ad una medesima banca dati in relazione alle diverse funzioni svolte dai propri operatori per il perseguimento della medesima finalita', modulando cosi' il livello di accesso ai dati. L'erogatore deve, infatti, far si' che sia consentita, per quanto piu' possibile, la segmentazione dei dati visualizzabili al fine di rendere consultabili dall'utente, anche in base al proprio profilo e in relazione al bacino di utenza del fruitore, esclusivamente i dati necessari rispetto alle finalita' in concreto perseguite. In altri termini la convenzione deve prevedere l'accesso alle sole informazioni pertinenti e non eccedenti rispetto alla finalita' istituzionale perseguita dalla convenzione stessa.

Particolare attenzione deve essere prestata, inoltre, nella scelta delle informazioni richieste per l'interrogazione diretta della banca dati, ovvero per l'invocazione dei web services, imponendo un set minimo di dati per l'individuazione puntuale del soggetto cui si riferiscono. Salvo eccezioni rigorosamente motivate e documentate nella convenzione, la risposta fornita all'interrogazione non deve, poi, contenere un elenco di soggetti.

2.3 Elenco aggiornato.

L'erogatore deve poi disporre in ogni momento di informazioni complete e strutturate sui fruitori autorizzati e sulle modalita' di accesso alle proprie banche dati.

A tal fine occorre pertanto che l'erogatore rediga un documento, mantenuto costantemente aggiornato, che riporti l'elenco delle banche dati accessibili, descrivendo per ogni fruitore le informazioni di cui ai punti a), b), c), di cui al precedente paragrafo 2.1, corredato delle informazioni relative ai formati dei dati disponibili a fruitori esterni ("tracciato record", schemi XML o altri formalismi).

2.4 Controlli annuali.

L'erogatore deve altresi' verificare, con cadenza periodica annuale, l'attualita' delle finalita' per cui ha concesso l'accesso ai fruitori, anche con riferimento al numero di utenze attive, inibendo gli accessi (autorizzazioni o singole utenze) non conformi a quanto stabilito nelle convenzioni.

3. Soggetti incaricati del trattamento.

3.1 Designazione responsabili e incaricati.

Per effetto dell'esecuzione della convenzione e della conseguente comunicazione dei dati personali, il fruitore, in quanto titolare del trattamento dei dati oggetto di comunicazione da parte dell'erogatore, ai sensi della normativa vigente in materia, deve dare attuazione a quanto previsto dagli artt. 29 e 30 del Codice della privacy, in materia di designazione degli incaricati del trattamento e eventuale designazione del responsabile del trattamento, garantendo che l'accesso ai dati sia consentito

esclusivamente a tali soggetti.

Il fruitore si impegna a comunicare all'erogatore, su richiesta motivata, l'elenco degli incaricati del trattamento autorizzati all'accesso ai dati (ad esempio, in caso di controlli sull'attualita' delle utenze la cui amministrazione e' demandata a gestori presso il fruitore, ovvero nel caso di cooperazione applicativa di cui al punto seguente).

Laddove i fruitori vogliano avvalersi di soggetti terzi (ad esempio, altra pubblica amministrazione o altro soggetto) al fine di realizzare servizi d'interscambio, previa apposita designazione dello stesso soggetto delegato come responsabile o, se persona fisica, anche incaricato del trattamento dei dati personali, devono darne comunicazione all'erogatore. Tale eventualita' deve essere, naturalmente, esplicitamente riportata nella convenzione.

3.2 Procedura di autenticazione e autorizzazione degli utenti.

a) Accessi via web

Nel caso in cui la modalita' di accesso prescelta preveda l'attribuzione di credenziali individuali (ad esempio, applicazione con accesso interattivo via web), le convenzioni devono predefinire una procedura per il rilascio delle utenze e la gestione delle autorizzazioni degli utenti che coinvolga attivamente le figure apicali degli uffici interessati e un unico supervisore (soggetto giuridicamente preposto all'individuazione degli utenti e dei profili). Il supervisore puo' anche non coincidere con il soggetto tecnicamente deputato alla materiale gestione delle utenze (direttamente o attraverso l'erogatore), ma deve rispondere del controllo sullo stesso.

Nel caso il sistema di accesso preveda la gestione diretta delle utenze da parte del fruitore, la convenzione deve prevedere l'individuazione di uno o piu' soggetti (coordinati tra loro) deputati alla materiale amministrazione delle utenze di coloro che sono stati autorizzati dal supervisore ad accedere alla banca dati. Tali gestori-amministratori devono essere preferibilmente scelti tra personale che abbia un rapporto stabile con il fruitore e devono essere adeguatamente formati in ordine alle modalita' di accesso alla banca dati e all'attivita' di autorizzazione degli utenti.

Occorre inoltre che venga assicurato un flusso di comunicazione tra il supervisore, il gestore e l'articolazione che si occupa della gestione delle risorse umane, al fine di procedere alla tempestiva revisione del profilo di abilitazione o alla disabilitazione dei soggetti preposti ad altre mansioni o che abbiano cessato il rapporto con l'ente, anche con apposite verifiche a cadenza almeno trimestrale. Il responsabile della convenzione individuato presso il fruitore deve effettuare periodicamente, con cadenza almeno annuale, anche in collaborazione con l'erogatore, una puntuale verifica sulla corretta attribuzione dei profili di autorizzazione e sull'attualita' delle utenze attive. Le convenzioni devono predefinire anche le soglie relative al numero di utenti abilitabili da ciascun fruitore.

L'elenco dei soggetti incaricati da abilitare all'accesso alla banca dati deve essere allegato alla convenzione, ovvero comunicato entro un termine ivi stabilito, e costantemente aggiornato dal responsabile della convenzione. Qualora la gestione degli utenti sia demandata al fruitore, la comunicazione potra' essere limitata agli utenti cui e' affidata la funzione di gestori dell'amministrazione delle utenze.

b) Cooperazione applicativa

I web services devono essere integrati soltanto in applicativi che gestiscono procedure amministrative volte al raggiungimento delle finalita' istituzionali per le quali e' consentita la comunicazione delle informazioni contenute nella banca dati. Devono essere, quindi, possibili unicamente accessi per le finalita' per le quali e' stata realizzata la convenzione alle sole informazioni pertinenti e non eccedenti rispetto alla finalita' istituzionale perseguita dalla convenzione.

In ogni caso, il fruitore deve garantire che i servizi resi disponibili dall'erogatore verranno esclusivamente integrati con il proprio sistema informativo e tali servizi non saranno resi disponibili a terzi per via informatica.

Le modalita' di accesso in cooperazione applicativa integrata negli applicativi utilizzati dal fruitore devono assicurare garanzie non inferiori a quelle individuate nel precedente punto a) attraverso idonee policy di sicurezza dei sistemi informativi dello stesso, che prevedano la presenza di una figura apicale (anche coadiuvata da un responsabile tecnico) a garanzia del rispetto dei presupposti per l'accesso stabiliti in convenzione, anche attraverso verifiche periodiche, in termini di:

gestione delle utenze;

profili di autorizzazione degli utenti in relazione ai dati ottenuti dall'erogatore mediante la piattaforma del fruitore;

misure di sicurezza.

Con riferimento all'identificazione dei soggetti incaricati dal fruitore che hanno accesso alla banca dati, al fine di consentire l'adeguato tracciamento delle operazioni compiute sui dati personali, il fruitore deve fornire all'erogatore, contestualmente ad ogni transazione effettuata, il codice identificativo dell'utenza che ha posto in essere l'operazione; il suddetto codice identificativo deve essere comunque riferito univocamente al singolo utente incaricato del trattamento che ha dato origine alla transazione; il fruitore, laddove vengano utilizzate utenze codificate (prive di elementi che rendano l'incaricato del trattamento direttamente identificabile), deve in ogni caso garantire anche all'erogatore la possibilita', su richiesta, di identificare l'utente nei casi in cui cio' si renda necessario.

3.3 Istruzioni e correttezza del trattamento.

Il fruitore deve utilizzare le informazioni acquisite esclusivamente per le finalita' dichiarate in convenzione, nel rispetto dei principi di pertinenza e non eccedenza, nonche' di indispensabilita', per i dati sensibili e giudiziari.

Il fruitore deve, altresi', garantire che non si verifichino divulgazioni, comunicazioni, cessioni a terzi, ne' in alcun modo riproduzioni dei dati nei casi diversi da quelli previsti dalla legge, stabilendo le condizioni per escludere il rischio di duplicazione delle basi dati realizzata anche attraverso l'utilizzo di strumenti automatizzati di interrogazione. A tal fine il fruitore si impegna ad utilizzare i sistemi di accesso ai dati in consultazione on line esclusivamente secondo le modalita' con cui sono stati resi disponibili e, di conseguenza, a non estrarre i dati per via automatica e massiva (attraverso ad esempio i cosiddetti "robot") allo scopo, ad esempio, di velocizzare le attivita' e creare autonome banche dati non conformi alle finalita' per le quali e' stato autorizzato all'accesso.

Il fruitore deve garantire, inoltre, che l'accesso ai dati verra' consentito esclusivamente al personale dipendente o a soggetti ad esso assimilati ovvero ad altri soggetti che siano stati parimenti designati dal fruitore quali incaricati o responsabili del trattamento dei dati, impartendo, ai sensi degli artt. 29 e 30 del Codice, precise e dettagliate istruzioni, richiamando la loro attenzione sulle responsabilita' connesse all'uso illegittimo dei dati, nonche' al corretto utilizzo delle funzionalita' dei collegamenti.

4. Dati sensibili e giudiziari.

In ogni caso, qualora sia indispensabile accedere a dati sensibili o giudiziari, questi devono essere opportunamente cifrati con algoritmi che garantiscano livelli di sicurezza adeguati al contesto ai sensi dell'art. 22, comma 6, del Codice.

In considerazione della delicatezza e della quantita' di informazioni scambiate, l'erogatore deve individuare le modalita' di trasferimento dei dati sensibili e giudiziari maggiormente idonee ad

assicurare la sicurezza dei collegamenti, prevedendo che il trasferimento dei dati idonei a rivelare lo stato di salute deve essere in ogni caso cifrato.

5. Misure di sicurezza.

Oltre a garantire il rispetto delle misure minime di sicurezza previste dall'artt. 33 e ss. Codice e dal relativo Allegato B, al fine di adempiere agli obblighi di sicurezza di cui all'art. 31 del Codice nella fruibilita' dei dati oggetto della convenzione (sia in caso di accessi via web che di cooperazione applicativa), l'erogatore e il fruitore devono assicurare che:

a. gli accessi alle banche dati avvengano soltanto tramite l'uso di postazioni di lavoro connesse alla rete Ip dell'ente autorizzato o dotate di certificazione digitale che identifichi univocamente la postazione di lavoro nei confronti dell'erogatore, anche attraverso procedure di accreditamento che consentano di definire reti di accesso sicure (circuiti privati virtuali);

b. laddove l'accesso alla banca dati dell'erogatore avvenga in forma di web application esposta su rete pubblica (Internet), l'applicazione sia realizzata con protocolli di sicurezza provvedendo ad asseverare l'identita' digitale dei server erogatori dei servizi tramite l'utilizzo di certificati digitali conformi alla norma tecnica ISO/IEC 9594-8:2014, emessi da una Certification Authority e riconosciuti dai piu' diffusi browser e sistemi operativi;

c. le procedure di registrazione avvengano con il riconoscimento diretto e l'identificazione certa dell'utente;

d. le regole di gestione delle credenziali di autenticazione prevedano, in ogni caso:

l'identificazione univoca di una persona fisica;

processi di emissione e distribuzione delle credenziali agli utenti in maniera sicura seguendo una procedura operativa prestabilita, o di accettazione di forme di autenticazione forte quali quelle che prevedono l'uso di one time password o di certificati di autenticazione (CNS o analoghi);

che le credenziali siano costituite da un dispositivo in possesso ed uso esclusivo dell'incaricato provvisto di pin o una coppia username/password, ovvero da credenziali che garantiscano analoghe condizioni di robustezza;

e. nel caso le credenziali siano costituite da una coppia username/password, siano adottate le seguenti politiche di gestione delle password:

la password, comunicata direttamente al singolo incaricato separatamente rispetto al codice per l'identificazione (user id), sia modificata dallo stesso al primo utilizzo e, successivamente, almeno ogni tre mesi e le ultime tre password non possano essere riutilizzate;

le password devono rispondere a requisiti di complessita' (almeno otto caratteri, uso di caratteri alfanumerici, lettere maiuscole e minuscole, caratteri estesi);

quando l'utente si allontana dal terminale, la sessione deve essere bloccata, anche attraverso eventuali meccanismi di time-out;

le credenziali devono essere bloccate a fronte di reiterati tentativi falliti di autenticazione;

f. devono essere sempre presenti misure di protezione perimetrali logico-fisiche, quali ad esempio firewall e reti private virtuali (VPN);

g. i sistemi software, i programmi utilizzati e la protezione antivirus devono essere costantemente aggiornati sia sui server che sulle postazioni di lavoro;

h. le misure di sicurezza devono periodicamente essere riconsiderate ed adeguate ai progressi tecnici e all'evoluzione dei rischi;

i. la procedura di autenticazione dell'utente deve essere protetta dal rischio di intercettazione delle credenziali da meccanismi crittografici di robustezza adeguata;

j. siano introdotti meccanismi volti a permettere il controllo degli accessi al fine di garantire che avvengano nell'ambito di intervalli temporali o di data predeterminati, eventualmente definiti sulla base delle esigenze d'ufficio;

k. in caso di accessi via web deve essere di regola esclusa la possibilita' di effettuare accessi contemporanei con le medesime credenziali da postazioni diverse;

l. anche al fine di ottemperare all'obbligo di comunicare al Garante entro 48 ore i casi di data breach, entrambi si impegnano a comunicare tempestivamente:

incidenti sulla sicurezza occorsi al proprio sistema di autenticazione qualora tali incidenti abbiano impatto direttamente o indirettamente nei processi di sicurezza afferenti la fruibilita' di dati oggetto di convenzione;

ogni eventuale esigenza di aggiornamento di stato degli utenti gestiti (nuovi inserimenti, disabilitazioni, cancellazioni) in caso di consultazione on line;

ogni modificazione tecnica od organizzativa del proprio dominio, che comporti l'impossibilita' di garantire l'applicazione delle regole di sopra riportate o la loro perdita di efficacia;

m. tutte le operazioni di trattamento di dati personali effettuate dagli utenti autorizzati, ivi comprese le utenze di tipo applicativo e sistemistico, devono essere adeguatamente tracciate. Al tal fine:

il fruitore deve fornire all'erogatore, contestualmente ad ogni transazione effettuata, il codice identificativo dell'utenza che ha posto in essere l'operazione;

il suddetto codice identificativo, anche nel caso in cui l'accesso avvenga attraverso sistemi di cooperazione applicativa, deve essere comunque riferito univocamente al singolo utente incaricato del trattamento che ha dato origine alla transazione;

il fruitore, laddove vengano utilizzate utenze codificate (prive di elementi che rendano l'incaricato del trattamento direttamente identificabile), deve in ogni caso garantire anche all'erogatore la possibilita', su richiesta, di identificare l'utente nei casi in cui cio' si renda necessario.

6. Controlli.

L'erogatore e il fruitore devono predisporre idonee procedure di audit sugli accessi alle banche dati, i cui esiti devono essere documentati secondo le modalita' definite nelle convenzioni.

In particolare, devono essere introdotte attivita' di audit basate sul monitoraggio statistico delle transazioni e su meccanismi di alert che individuino comportamenti anomali o a rischio.

A tal fine, nelle applicazioni volte all'uso interattivo da parte di incaricati deve essere inserito un campo per l'indicazione obbligatoria del numero di riferimento della pratica (ad es. numero del protocollo o del verbale) nell'ambito della quale viene effettuata la consultazione.

Le suddette procedure devono, inoltre, prevedere la verifica periodica, anche a campione, del rispetto dei presupposti stabiliti nelle convenzioni che autorizzano l'accesso (quali, in particolare, la rispondenza delle interrogazioni ad una precisa finalita' amministrativa).

7. Casi particolari.

Come sopra ricordato, e' compito dell'erogatore valutare l'introduzione di eventuali ulteriori misure e accorgimenti al fine di salvaguardare la sicurezza dei propri sistemi informativi, anche in considerazione delle caratteristiche delle banche dati accessibili attraverso la convenzione (ad esempio, delicatezza e rilevanza delle informazioni accedute, rilevanti dimensioni della banca dati o del numero di utenti o volume di trasferimenti). Tali misure possono riguardare, in particolare:

l'individuazione di tassative modalita' di accesso alle banche dati;

la gestione diretta da parte dell'erogatore dei profili di abilitazione, con la conoscenza dei dati identificativi dei soggetti autorizzati all'accesso alla banca dati per la realizzazione delle finalita' istituzionali dichiarate nella convenzione;

l'utilizzo di strumenti di strong authentication per l'autenticazione informatica di particolari categorie di utenti;

in caso di accessi via web o applicazioni software:

nella prima schermata successiva al collegamento con la banca dati, siano visualizzabili le informazioni relative all'ultima sessione effettuata con le stesse credenziali (almeno con l'indicazione di data, ora e indirizzo di rete da cui e' stata effettuata la precedente connessione);

le informazioni di cui al punto precedente devono essere riportate anche relativamente alla sessione corrente;

la verifica di accessi anomali attraverso strumenti di business intelligence per monitorare gli accessi attraverso i log relativi a tutti gli attuali e futuri applicativi utilizzati da parte dei fruitori, ovvero attraverso specifiche procedure di audit dell'erogatore presso il fruitore.

ALLEGATO *1*

GARANTE
PER LA PROTEZIONE DEI
DATI PERSONALI

VIOLAZIONE DI DATI PERSONALI

MODELLO DI COMUNICAZIONE AL GARANTE

Secondo quanto prescritto dal Provvedimento del 2 luglio 2015, le amministrazioni pubbliche sono tenute a comunicare al Garante all'indirizzo: **databreach.pa@pec.gpdp.it** le violazioni dei dati personali (*data breach*) che si verificano nell'ambito delle banche dati (qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti, art. 4, comma 1, lett. *p* del Codice) di cui sono titolari.

La comunicazione deve essere effettuata entro 48 ore dalla conoscenza del fatto, compilando il modulo che segue.

Amministrazione titolare del trattamento

Denominazione o ragione sociale _____

Provincia _____ **Comune** _____

Cap _____ **Indirizzo** _____

Nome persona fisica addetta alla comunicazione _____

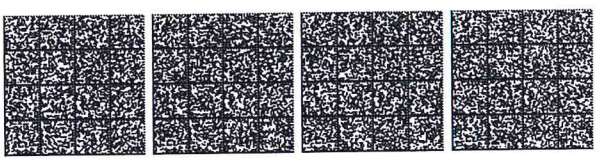
Cognome persona fisica addetta alla comunicazione _____

Funzione rivestita _____

Indirizzo PEC e/o EMAIL per eventuali comunicazioni _____

Recapito telefonico per eventuali comunicazioni _____

Eventuali Contatti (altre informazioni) _____



Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati?

- ☐ Il _____
- ☐ Tra il _____ e il _____
- ☐ In un tempo non ancora determinato
- ☐ E' possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio

Tipo di violazione

- ☐ Lettura (presumibilmente i dati non sono stati copiati)
- ☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
- ☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- ☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- ☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
- ☐ Altro :

Dispositivo oggetto della violazione

☐ Computer
☐ Rete
☐ Dispositivo mobile
☐ File o parte di un file
☐ Strumento di *backup*
☐ Documento cartaceo
☐ Altro :

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

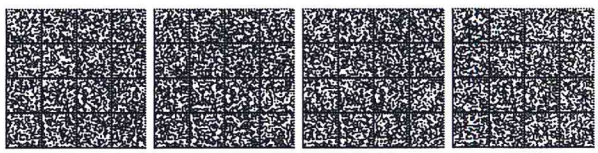
☐ N. _____ persone
☐ Circa _____ persone
☐ Un numero (ancora) sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

☐ Dati anagrafici/codice fiscale
☐ Dati di accesso e di identificazione (*user name*, *password*, *customer ID*, altro)
☐ Dati relativi a minori
☐ Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
☐ Dati personali idonei a rivelare lo stato di salute e la vita sessuale
☐ Dati giudiziari
☐ Copia per immagine su supporto informatico di documenti analogici
☐ Ancora sconosciuto
☐ Altro :

Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del titolare)?

☐ Basso/trascurabile
☐ Medio
☐ Alto
☐ Molto alto



Misure tecniche e organizzative applicate ai dati oggetto di violazione

La violazione è stata comunicata anche agli interessati?

☐ Sì, è stata comunicata il

☐ No, perché _____

Qual è il contenuto della comunicazione resa agli interessati?

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

(Allegato 2)

Allegato 2

Misure necessarie

1. Modalita' d'accesso.

Le pubbliche amministrazioni che intendono rendere fruibili diverse tipologie di dati da altre pubbliche amministrazioni, tenuto conto degli obiettivi di carattere generale perseguiti dal Cad e dell'attuale quadro infrastrutturale disponibile sul territorio, utilizzano le seguenti opzioni tecniche:

accesso via web, attraverso il sito istituzionale dell'erogatore, un sito tematico appositamente predisposto o altre applicazioni software;

accesso in modalita' di cooperazione applicativa, componente del sistema pubblico di connettivita' finalizzata all'interazione tra i sistemi informatici delle pubbliche amministrazioni per garantire l'integrazione dei metadati, delle informazioni e dei procedimenti amministrativi.

Ferme restando le modalita' di accesso telematico definite al punto precedente, che devono considerarsi quelle di riferimento ai fini dell'attuazione delle norme in materia di fruibilita' dei dati, le amministrazioni possono utilizzare modalita' alternative, laddove si presentino documentabili vantaggi economici o la situazione infrastrutturale e organizzativa non consenta l'adozione di quelle sopra riportate. Le predette circostanze devono essere adeguatamente documentate. In tali casi, le modalita' di accesso telematico prevedibili sono:

la posta elettronica certificata, nei casi specifici, quando la periodicita' di acquisizione del dato e' limitata (in linea di massima una volta all'anno o meno) e la quantita' dei dati da acquisire e' contenuta;

soluzioni di "Trasferimento di File" in modalita' FTP "sicuro" o equivalente dal punto di vista della sicurezza del trasporto, qualora preesistenti investimenti, la natura stessa delle richieste e le specifiche condizioni facciano propendere per tale soluzione garantendo la cifratura del canale di trasmissione dei dati (ad esempio, utilizzando meccanismi quali le reti private virtuali o la cifratura delle sessioni di trasferimento dei dati).

2. Presupposti per la comunicazione di dati personali.

La convenzione (ovvero qualsivoglia atto bilaterale stipulato tra erogatore e fruitore al fine di stabilire le condizioni e le modalita' di accesso ai dati) e' lo strumento in cui le amministrazioni possono stabilire le garanzie - anche nei confronti dello stesso erogatore - a tutela del trattamento dei dati personali e dell'utilizzo dei sistemi informativi.

Di seguito vengono pertanto individuati misure e accorgimenti da attuare al fine di assicurare la correttezza del trattamento e di ridurre rischi nell'utilizzo dei dati personali.

In ogni caso l'erogatore, al fine di salvaguardare la sicurezza dei propri sistemi informativi, anche in considerazione delle caratteristiche delle banche dati accessibili attraverso la convenzione, e' tenuto a valutare l'introduzione di ulteriori strumenti volti a gestire i profili di autorizzazione, verificare accessi anomali, tracciare le operazioni di accesso, ovvero individuare tassative modalita' di accesso alle banche dati, dandone conto nella convenzione (art. 31 del Codice).

2.1 Verifiche preliminari a cura dell'erogatore.

L'erogatore prima di stipulare ogni singola convenzione per l'accesso alle proprie banche dati in via telematica deve verificare:

a) la base normativa che legittima il fruitore ad accedere alle proprie banche dati (per i dati diversi da quelli di sensibili e giudiziali: norma di legge o di regolamento, ovvero previa comunicazione al Garante ai sensi dell'art. 19, comma 2 del Codice, qualora manchi una norma di legge o di regolamento e il flusso di dati risulti necessario per lo svolgimento delle proprie funzioni istituzionali; per i dati sensibili e giudiziari: la norma di legge che autorizzi il trattamento e l'individuazione nella stessa, o in atto di natura regolamentare adottato in conformita' al parere del Garante, dei tipi di dati e le operazioni eseguibili);

b) la finalita' istituzionale perseguita dal fruitore (ad esempio controllo sulle dichiarazioni sostitutive) e la natura e la qualita' dei dati richiesti, selezionando accuratamente le informazioni personali contenute nelle banche dati a cui dare accesso;

c) la modalita' telematica di accesso alle banche dati piu' idonea rispetto alle finalita', alla natura e alla quantita' dei dati, alle caratteristiche anche infrastrutturali e organizzative del fruitore, al volume e alla frequenza dei trasferimenti, al numero di soggetti abilitati all'accesso.

2.2 Selezione dei dati.

La selezione delle informazioni personali oggetto di accesso deve avvenire nel rispetto dei principi di pertinenza e non eccedenza in relazione a ciascuna delle finalita' perseguite dal fruitore. Rispetto ad una medesima banca dati devono essere, infatti, prefigurati diversi livelli e modalita' di accesso che offrano al fruitore unicamente i dati necessari per le proprie esigenze istituzionali.

Le modalita' di accesso alle banche dati devono essere, pertanto, configurate offrendo un livello minimo di accesso ai dati, anche limitando i risultati delle interrogazioni a valori di tipo booleano (ad es., web services che forniscono un risultato di tipo vero/falso nel caso di controlli sull'esistenza o sulla correttezza di un dato oggetto di autocertificazione). Livelli di accesso gradualmente piu' ampi possono essere autorizzati soltanto a fronte di documentate esigenze del fruitore da indicare in convenzione.

E' chiaro, inoltre, che per ciascun fruitore possono essere individuate piu' modalita' di accesso ad una medesima banca dati in relazione alle diverse funzioni svolte dai propri operatori per il perseguimento della medesima finalita', modulando cosi' il livello di accesso ai dati. L'erogatore deve, infatti, far si' che sia consentita, per quanto piu' possibile, la segmentazione dei dati visualizzabili al fine di rendere consultabili dall'utente, anche in base al proprio profilo e in relazione al bacino di utenza del fruitore, esclusivamente i dati necessari rispetto alle finalita' in concreto perseguite. In altri termini la convenzione deve prevedere l'accesso alle sole informazioni pertinenti e non eccedenti rispetto alla finalita' istituzionale perseguita dalla convenzione stessa.

Particolare attenzione deve essere prestata, inoltre, nella scelta delle informazioni richieste per l'interrogazione diretta della banca dati, ovvero per l'invocazione dei web services, imponendo un set minimo di dati per l'individuazione puntuale del soggetto cui si riferiscono. Salvo eccezioni rigorosamente motivate e documentate nella convenzione, la risposta fornita all'interrogazione non deve, poi, contenere un elenco di soggetti.

2.3 Elenco aggiornato.

L'erogatore deve poi disporre in ogni momento di informazioni complete e strutturate sui fruitori autorizzati e sulle modalita' di

accesso alle proprie banche dati.

A tal fine occorre pertanto che l'erogatore rediga un documento, mantenuto costantemente aggiornato, che riporti l'elenco delle banche dati accessibili, descrivendo per ogni fruitore le informazioni di cui ai punti a), b), c), di cui al precedente paragrafo 2.1, corredato delle informazioni relative ai formati dei dati disponibili a fruitori esterni ("tracciato record", schemi XML o altri formalismi).

2.4 Controlli annuali.

L'erogatore deve altresi' verificare, con cadenza periodica annuale, l'attualita' delle finalita' per cui ha concesso l'accesso ai fruitori, anche con riferimento al numero di utenze attive, inibendo gli accessi (autorizzazioni o singole utenze) non conformi a quanto stabilito nelle convenzioni.

3. Soggetti incaricati del trattamento.

3.1 Designazione responsabili e incaricati.

Per effetto dell'esecuzione della convenzione e della conseguente comunicazione dei dati personali, il fruitore, in quanto titolare del trattamento dei dati oggetto di comunicazione da parte dell'erogatore, ai sensi della normativa vigente in materia, deve dare attuazione a quanto previsto dagli artt. 29 e 30 del Codice della privacy, in materia di designazione degli incaricati del trattamento e eventuale designazione del responsabile del trattamento, garantendo che l'accesso ai dati sia consentito esclusivamente a tali soggetti.

Il fruitore si impegna a comunicare all'erogatore, su richiesta motivata, l'elenco degli incaricati del trattamento autorizzati all'accesso ai dati (ad esempio, in caso di controlli sull'attualita' delle utenze la cui amministrazione e' demandata a gestori presso il fruitore, ovvero nel caso di cooperazione applicativa di cui al punto seguente).

Laddove i fruitori vogliano avvalersi di soggetti terzi (ad esempio, altra pubblica amministrazione o altro soggetto) al fine di realizzare servizi d'interscambio, previa apposita designazione dello stesso soggetto delegato come responsabile o, se persona fisica, anche incaricato del trattamento dei dati personali, devono darne comunicazione all'erogatore. Tale eventualita' deve essere, naturalmente, esplicitamente riportata nella convenzione.

3.2 Procedura di autenticazione e autorizzazione degli utenti.

a) Accessi via web

Nel caso in cui la modalita' di accesso prescelta preveda l'attribuzione di credenziali individuali (ad esempio, applicazione con accesso interattivo via web), le convenzioni devono predefinire una procedura per il rilascio delle utenze e la gestione delle autorizzazioni degli utenti che coinvolga attivamente le figure apicali degli uffici interessati e un unico supervisore (soggetto giuridicamente preposto all'individuazione degli utenti e dei profili). Il supervisore puo' anche non coincidere con il soggetto tecnicamente deputato alla materiale gestione delle utenze (direttamente o attraverso l'erogatore), ma deve rispondere del controllo sullo stesso.

Nel caso il sistema di accesso preveda la gestione diretta delle utenze da parte del fruitore, la convenzione deve prevedere l'individuazione di uno o piu' soggetti (coordinati tra loro) deputati alla materiale amministrazione delle utenze di coloro che sono stati autorizzati dal supervisore ad accedere alla banca dati. Tali gestori-amministratori devono essere preferibilmente scelti tra personale che abbia un rapporto stabile con il fruitore e devono essere adeguatamente formati in ordine alle modalita' di accesso alla

banca dati e all'attivita' di autorizzazione degli utenti.

Occorre inoltre che venga assicurato un flusso di comunicazione tra il supervisore, il gestore e l'articolazione che si occupa della gestione delle risorse umane, al fine di procedere alla tempestiva revisione del profilo di abilitazione o alla disabilitazione dei soggetti preposti ad altre mansioni o che abbiano cessato il rapporto con l'ente, anche con apposite verifiche a cadenza almeno trimestrale. Il responsabile della convenzione individuato presso il fruitore deve effettuare periodicamente, con cadenza almeno annuale, anche in collaborazione con l'erogatore, una puntuale verifica sulla corretta attribuzione dei profili di autorizzazione e sull'attualita' delle utenze attive. Le convenzioni devono predefinire anche le soglie relative al numero di utenti abilitabili da ciascun fruitore.

L'elenco dei soggetti incaricati da abilitare all'accesso alla banca dati deve essere allegato alla convenzione, ovvero comunicato entro un termine ivi stabilito, e costantemente aggiornato dal responsabile della convenzione. Qualora la gestione degli utenti sia demandata al fruitore, la comunicazione potra' essere limitata agli utenti cui e' affidata la funzione di gestori dell'amministrazione delle utenze.

b) Cooperazione applicativa

I web services devono essere integrati soltanto in applicativi che gestiscono procedure amministrative volte al raggiungimento delle finalita' istituzionali per le quali e' consentita la comunicazione delle informazioni contenute nella banca dati. Devono essere, quindi, possibili unicamente accessi per le finalita' per le quali e' stata realizzata la convenzione alle sole informazioni pertinenti e non eccedenti rispetto alla finalita' istituzionale perseguita dalla convenzione.

In ogni caso, il fruitore deve garantire che i servizi resi disponibili dall'erogatore verranno esclusivamente integrati con il proprio sistema informativo e tali servizi non saranno resi disponibili a terzi per via informatica.

Le modalita' di accesso in cooperazione applicativa integrata negli applicativi utilizzati dal fruitore devono assicurare garanzie non inferiori a quelle individuate nel precedente punto a) attraverso idonee policy di sicurezza dei sistemi informativi dello stesso, che prevedano la presenza di una figura apicale (anche coadiuvata da un responsabile tecnico) a garanzia del rispetto dei presupposti per l'accesso stabiliti in convenzione, anche attraverso verifiche periodiche, in termini di:

gestione delle utenze;

profili di autorizzazione degli utenti in relazione ai dati ottenuti dall'erogatore mediante la piattaforma del fruitore;

misure di sicurezza.

Con riferimento all'identificazione dei soggetti incaricati dal fruitore che hanno accesso alla banca dati, al fine di consentire l'adeguato tracciamento delle operazioni compiute sui dati personali, il fruitore deve fornire all'erogatore, contestualmente ad ogni transazione effettuata, il codice identificativo dell'utenza che ha posto in essere l'operazione; il suddetto codice identificativo deve essere comunque riferito univocamente al singolo utente incaricato del trattamento che ha dato origine alla transazione; il fruitore, laddove vengano utilizzate utenze codificate (prive di elementi che rendano l'incaricato del trattamento direttamente identificabile), deve in ogni caso garantire anche all'erogatore la possibilita', su richiesta, di identificare l'utente nei casi in cui cio' si renda necessario.

3.3 Istruzioni e correttezza del trattamento.

Il fruitore deve utilizzare le informazioni acquisite esclusivamente per le finalita' dichiarate in convenzione, nel rispetto dei principi di pertinenza e non eccedenza, nonche' di indispensabilita', per i dati sensibili e giudiziari.

Il fruitore deve, altresi', garantire che non si verifichino divulgazioni, comunicazioni, cessioni a terzi, ne' in alcun modo riproduzioni dei dati nei casi diversi da quelli previsti dalla legge, stabilendo le condizioni per escludere il rischio di duplicazione delle basi dati realizzata anche attraverso l'utilizzo di strumenti automatizzati di interrogazione. A tal fine il fruitore si impegna ad utilizzare i sistemi di accesso ai dati in consultazione on line esclusivamente secondo le modalita' con cui sono stati resi disponibili e, di conseguenza, a non estrarre i dati per via automatica e massiva (attraverso ad esempio i cosiddetti "robot") allo scopo, ad esempio, di velocizzare le attivita' e creare autonome banche dati non conformi alle finalita' per le quali e' stato autorizzato all'accesso.

Il fruitore deve garantire, inoltre, che l'accesso ai dati verra' consentito esclusivamente al personale dipendente o a soggetti ad esso assimilati ovvero ad altri soggetti che siano stati parimenti designati dal fruitore quali incaricati o responsabili del trattamento dei dati, impartendo, ai sensi degli artt. 29 e 30 del Codice, precise e dettagliate istruzioni, richiamando la loro attenzione sulle responsabilita' connesse all'uso illegittimo dei dati, nonche' al corretto utilizzo delle funzionalita' dei collegamenti.

4. Dati sensibili e giudiziari.

In ogni caso, qualora sia indispensabile accedere a dati sensibili o giudiziari, questi devono essere opportunamente cifrati con algoritmi che garantiscano livelli di sicurezza adeguati al contesto ai sensi dell'art. 22, comma 6, del Codice.

In considerazione della delicatezza e della quantita' di informazioni scambiate, l'erogatore deve individuare le modalita' di trasferimento dei dati sensibili e giudiziari maggiormente idonee ad assicurare la sicurezza dei collegamenti, prevedendo che il trasferimento dei dati idonei a rivelare lo stato di salute deve essere in ogni caso cifrato.

5. Misure di sicurezza.

Oltre a garantire il rispetto delle misure minime di sicurezza previste dall'artt. 33 e ss. Codice e dal relativo Allegato B, al fine di adempiere agli obblighi di sicurezza di cui all'art. 31 del Codice nella fruibilita' dei dati oggetto della convenzione (sia in caso di accessi via web che di cooperazione applicativa), l'erogatore e il fruitore devono assicurare che:

a. gli accessi alle banche dati avvengano soltanto tramite l'uso di postazioni di lavoro connesse alla rete Ip dell'ente autorizzato o dotate di certificazione digitale che identifichi univocamente la postazione di lavoro nei confronti dell'erogatore, anche attraverso procedure di accreditamento che consentano di definire reti di accesso sicure (circuiti privati virtuali);

b. laddove l'accesso alla banca dati dell'erogatore avvenga in forma di web application esposta su rete pubblica (Internet), l'applicazione sia realizzata con protocolli di sicurezza provvedendo ad asseverare l'identita' digitale dei server erogatori dei servizi tramite l'utilizzo di certificati digitali conformi alla norma tecnica ISO/IEC 9594-8:2014, emessi da una Certification Authority e riconosciuti dai piu' diffusi browser e sistemi operativi;

c. le procedure di registrazione avvengano con il riconoscimento diretto e l'identificazione certa dell'utente;

d. le regole di gestione delle credenziali di autenticazione prevedano, in ogni caso:

l'identificazione univoca di una persona fisica;

processi di emissione e distribuzione delle credenziali agli utenti in maniera sicura seguendo una procedura operativa prestabilita, o di accettazione di forme di autenticazione forte quali quelle che prevedono l'uso di one time password o di certificati di autenticazione (CNS o analoghi);

che le credenziali siano costituite da un dispositivo in possesso ed uso esclusivo dell'incaricato provvisto di pin o una coppia username/password, ovvero da credenziali che garantiscano analoghe condizioni di robustezza;

e. nel caso le credenziali siano costituite da una coppia username/password, siano adottate le seguenti politiche di gestione delle password:

la password, comunicata direttamente al singolo incaricato separatamente rispetto al codice per l'identificazione (user id), sia modificata dallo stesso al primo utilizzo e, successivamente, almeno ogni tre mesi e le ultime tre password non possano essere riutilizzate;

le password devono rispondere a requisiti di complessita' (almeno otto caratteri, uso di caratteri alfanumerici, lettere maiuscole e minuscole, caratteri estesi);

quando l'utente si allontana dal terminale, la sessione deve essere bloccata, anche attraverso eventuali meccanismi di time-out;

le credenziali devono essere bloccate a fronte di reiterati tentativi falliti di autenticazione;

f. devono essere sempre presenti misure di protezione perimetrali logico-fisiche, quali ad esempio firewall e reti private virtuali (VPN);

g. i sistemi software, i programmi utilizzati e la protezione antivirus devono essere costantemente aggiornati sia sui server che sulle postazioni di lavoro;

h. le misure di sicurezza devono periodicamente essere riconsiderate ed adeguate ai progressi tecnici e all'evoluzione dei rischi;

i. la procedura di autenticazione dell'utente deve essere protetta dal rischio di intercettazione delle credenziali da meccanismi crittografici di robustezza adeguata;

j. siano introdotti meccanismi volti a permettere il controllo degli accessi al fine di garantire che avvengano nell'ambito di intervalli temporali o di data predeterminati, eventualmente definiti sulla base delle esigenze d'ufficio;

k. in caso di accessi via web deve essere di regola esclusa la possibilita' di effettuare accessi contemporanei con le medesime credenziali da postazioni diverse;

l. anche al fine di ottemperare all'obbligo di comunicare al Garante entro 48 ore i casi di data breach, entrambi si impegnano a comunicare tempestivamente:

incidenti sulla sicurezza occorsi al proprio sistema di autenticazione qualora tali incidenti abbiano impatto direttamente o indirettamente nei processi di sicurezza afferenti la fruibilita' di dati oggetto di convenzione;

ogni eventuale esigenza di aggiornamento di stato degli utenti gestiti (nuovi inserimenti, disabilitazioni, cancellazioni) in caso di consultazione on line;

ogni modificazione tecnica od organizzativa del proprio dominio, che comporti l'impossibilita' di garantire l'applicazione delle regole di sopra riportate o la loro perdita di efficacia;

m. tutte le operazioni di trattamento di dati personali effettuate dagli utenti autorizzati, ivi comprese le utenze di tipo applicativo e sistemistico, devono essere adeguatamente tracciate. Al tal fine:

il fruitore deve fornire all'erogatore, contestualmente ad ogni transazione effettuata, il codice identificativo dell'utenza che ha posto in essere l'operazione;

il suddetto codice identificativo, anche nel caso in cui l'accesso avvenga attraverso sistemi di cooperazione applicativa, deve essere comunque riferito univocamente al singolo utente incaricato del trattamento che ha dato origine alla transazione;

il fruitore, laddove vengano utilizzate utenze codificate (prive di elementi che rendano l'incaricato del trattamento direttamente identificabile), deve in ogni caso garantire anche all'erogatore la possibilita', su richiesta, di identificare l'utente nei casi in cui cio' si renda necessario.

6. Controlli.

L'erogatore e il fruitore devono predisporre idonee procedure di audit sugli accessi alle banche dati, i cui esiti devono essere documentati secondo le modalita' definite nelle convenzioni.

In particolare, devono essere introdotte attivita' di audit basate sul monitoraggio statistico delle transazioni e su meccanismi di alert che individuino comportamenti anomali o a rischio.

A tal fine, nelle applicazioni volte all'uso interattivo da parte di incaricati deve essere inserito un campo per l'indicazione obbligatoria del numero di riferimento della pratica (ad es. numero del protocollo o del verbale) nell'ambito della quale viene effettuata la consultazione.

Le suddette procedure devono, inoltre, prevedere la verifica periodica, anche a campione, del rispetto dei presupposti stabiliti nelle convenzioni che autorizzano l'accesso (quali, in particolare, la rispondenza delle interrogazioni ad una precisa finalita' amministrativa).

7. Casi particolari.

Come sopra ricordato, e' compito dell'erogatore valutare l'introduzione di eventuali ulteriori misure e accorgimenti al fine di salvaguardare la sicurezza dei propri sistemi informativi, anche in considerazione delle caratteristiche delle banche dati accessibili attraverso la convenzione (ad esempio, delicatezza e rilevanza delle informazioni accedute, rilevanti dimensioni della banca dati o del numero di utenti o volume di trasferimenti). Tali misure possono riguardare, in particolare:

l'individuazione di tassative modalita' di accesso alle banche dati;

la gestione diretta da parte dell'erogatore dei profili di abilitazione, con la conoscenza dei dati identificativi dei soggetti autorizzati all'accesso alla banca dati per la realizzazione delle finalita' istituzionali dichiarate nella convenzione;

l'utilizzo di strumenti di strong authentication per l'autenticazione informatica di particolari categorie di utenti;

in caso di accessi via web o applicazioni software:

nella prima schermata successiva al collegamento con la banca dati, siano visualizzabili le informazioni relative all'ultima sessione effettuata con le stesse credenziali (almeno con l'indicazione di data, ora e indirizzo di rete da cui e' stata effettuata la precedente connessione);

le informazioni di cui al punto precedente devono essere riportate anche relativamente alla sessione corrente;

la verifica di accessi anomali attraverso strumenti di business

intelligence per monitorare gli accessi attraverso i log relativi a tutti gli attuali e futuri applicativi utilizzati da parte dei fruitori, ovvero attraverso specifiche procedure di audit dell'erogatore presso il fruitore.