Vademecum sul *Data Breach*

Gentile Interessato,

in data 06.07.2021 si è verificata una violazione dei dati personali (c.d. "Data Breach") che potrebbe aver coinvolto anche i Suoi dati. Il presente documento è volto ad illustrarLe in maniera chiara e comprensibile la natura di tale Data Breach, le sue implicazioni e le possibili azioni di rimedio applicabili da Lei o già applicate da Fidi Nordest, così come definito dal Regolamento (UE) 2016/679, "Regolamento Generale sulla Protezione dei Dati" ("GDPR") agli artt. 33-34. Nello specifico, questo Vademecum contiene, nella forma di FAQ ("Frequently Asked Questions", ovvero le "domande più comuni"), le seguenti informazioni:

- *Il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;*
- *Le probabili conseguenze della violazione dei dati personali;*
- *Le misure adottate da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.*

INDICE

FAQ

Cos'è un "dato personale"?

Secondo l'art. 4(1) del Regolamento (UE) 2016/679, "Regolamento Generale sulla Protezione dei Dati" ("**GDPR**"), per dato personale si intende "*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale"*.

Stante questa definizione, sono considerati dati personali nome e cognome, codice fiscale, l'IBAN, l'indirizzo e-mail e fisico e, in generale tutti quelle informazioni che possono essere ricondotte direttamente o indirettamente ad una persona fisica.

Cos'è un *"data breach"* e cosa è acceduto a luglio?

Un *"data breach"* è una violazione dei dati personali, ovvero una tipologia di incidente di sicurezza che ha ad oggetto dati personali. Il *data breach* è definito dal GDPR all'art. 4 come "*una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*". Le conseguenze illustrate vanno intese in forma disgiuntiva, ovvero basta l'occorrenza di una sola per determinare un data breach. Ad esempio, la "distruzione" dei dati può essere qualificata come data breach.

Si ha la "distruzione" dei dati quando gli stessi non esistono più o non si trovano più in una forma utilizzabile. Con "perdita" dei dati personali si intende la circostanza in cui i dati potrebbero comunque esistere, ma se ne sia perso il controllo o l'accesso, oppure non se ne sia più in possesso. Infine, "la modifica, la divulgazione non autorizzata o l'accesso ai dati personali" accade quando soggetti non autorizzati sono messi nella situazione di poter ricevere, accedere o a modificare tali dati.

Nel caso in questione, la violazione ha interessato i soggetti (clienti, dipendenti, consulenti, utenti) i cui dati personali erano nei sistemi di Fidi Nordest e si è verificata a causa di un attacco esterno di un gruppo di cybercriminali.

Più nello specifico, a causa vulnerabilità di un applicativo informativo, il 6 luglio 2021 i cybercriminali sono entrati ed hanno installato un *ransomware* all'interno di uno dei server di Fidi Nordest rendendone impossibile l'accesso. Fidi Nordest è intervenuta tempestivamente il giorno stesso dall'attacco, ripristinando i dati presenti nel server e adottando tutte le misure ritenute necessarie per evitare che l'evento possa ripetersi in futuro.

Che tipologie di informazioni sono state rese disponibili durante il data breach?

Per il breve periodo in cui il server di Fidi Nordest è stato oggetto di attacco esterno, potevano essere presenti le seguenti tipologie di dati personali:

- Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale)
- Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
- Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)

- Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza
- Dati di profilazione
- Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
- Dati che rivelino l'appartenenza sindacale.

Più nello specifico, potevamo essere presenti:

- Per i clienti: Carta Identità' clienti; C.F; Unico; Bilanci; Eurisc; Visure; Fideiussioni; Dichiarazione Iva, Iscrizione a socio; Indirizzo e-mail; Pec e recapiti telefonici; Strategie aziendali per Covid; Ppt; Sos.
- Per i dipendenti: iban; eventuali dati personali copiati in pc aziendale dal singolo dipendente in contrasto con le policy aziendali; appartenenza categorie protette; adesione fondi pensioni; premi e passaggi di livello; c.v. e candidature; contenziosi con dipendenti; congedi parentali; carichi pendenti degli esponenti aziendali.

Il *Data Breach* per Lei ha avuto luogo esclusivamente nel caso in cui tali dati fossero presenti all'interno dei nostri sistemi.

Quali sono le conseguenze per la violazione di questi dati?

Dopo un Data Breach, è lecito chiedersi cosa succede alla riservatezza dei propri dati e come questi possono essere utilizzati dai soggetti che ne vengono in possesso.

È doveroso precisare che, nel caso accaduto lo scorso luglio, il tempo di accesso da parte degli attaccanti esterni ai dati presenti nel server di Fidi Nordest non pare essere tale da ritenere ragionevolmente che vi sia stata una possibile estrazione di dati personali, benché non ve ne sia la certezza. Tra le possibili conseguenze vi potrebbero essere il rischio di disservizi, tentativi di frode o furti d'identità. In questi mesi Fidi Nordest ha mantenuto alto il livello di attenzione e monitoraggio senza ricevere segnalazioni di tali eventi.

Si riporta di seguito alcune conseguenze che potrebbero accadere con l'accesso a determinati dati personali.

Se i dati personali fossero stati copiati, un cybercriminale potrebbe ipoteticamente cercare di **ricavare le credenziali di autenticazione** (ovvero le password) dei soggetti che hanno subito la violazione per l'accesso a diversi siti web (inclusi i social network): ciò risulterebbe particolarmente verosimile qualora le password consistano in combinazioni di informazioni personali come nomi, indirizzi, date di nascita, numeri di telefono o informazioni finanziarie.

Si rammenta, comunque, che chiunque si introduca abusivamente all'interno di un sistema informatico o telematico protetto da misure di sicurezza quali la password e vi si mantenga contro la volontà di chi ha il diritto di escluderlo pone in essere una condotta penalmente rilevante, punita con la reclusione fino a tre anni (Fidi Nordest ha invero esposto querela contro ignoti).

Inoltre, se i dati ricavati dal server dovessero consentire di risalire a credenziali, chi riproduce, diffonde, comunica o consegna codici, password e mezzi idonei all'accesso ad un sistema informatico protetto commette, anche in questo caso, un reato punito con la reclusione sino ad un anno ex art. 615 quater del codice penale.

Un'altra minaccia, qualora alcuni dati personali fossero stati carpiti da cybercriminali, sarebbe quella relativa al ***phishing*** e allo ***spear phishing***: il *phishing* è un tentativo di frode generalmente condotto tramite invio di e-mail contenenti un testo che induce il destinatario a compiere delle azioni come cliccare su un link, aprire un allegato, inviare un pagamento, rinviare documentazione. Si tratta di uno stratagemma che può indurre i destinatari a rivelare informazioni personali o a infettare i propri dispositivi con pericolosi *malware* (un termine generico che descrive un programma/codice dannoso che mette a rischio un sistema).

Lo *spear phishing* è una forma di adescamento: in senso figurato, come richiamato dal termine inglese *spear* che significa "fiocina", si tratta di un "pescatore che vuole prendere proprio quel pesce". L'oggetto dell'attacco viene accuratamente selezionato e studiato attraverso una raccolta di informazioni. Nello *spear phishing*, le e-mail inviate sono preparate *ad hoc* per risultare credibili e indurre le vittime in errore, citando particolari conosciuti alla vittima o nomi di persone reali vicine alla vittima. Nel caso in esame, i dati presenti nel server potrebbero rappresentare una fonte preziosa di informazioni per preparare un attacco di *spear phishing*, in quanto contengono diversi dati finanziari ipoteticamente utili a permettere a malintenzionati di spacciarsi per un ente di credito o per un dipendente di banca.

In caso di dubbi sull'identità o veridicità di una comunicazione (chiamata/e-mail/pec) di Fidi Nordest, La invitiamo a contattare i recapiti indicati nella FAQ "A chi posso rivolgermi per avere più informazioni relativamente all'accaduto o a questo documento?".

Nella FAQ **"Cosa posso fare per proteggermi dalle minacce descritte sopra?"** qui di seguito può trovare invece utili suggerimenti per aumentare la sua sicurezza, a prescindere dalla violazione accaduta.

Cosa posso fare per proteggermi dalle minacce descritte sopra?

Qualora vengano utilizzate password legate ad informazioni personali, quali codice fiscale, nome, cognome, data di nascita, indirizzo, numero di telefono, etc., è opportuno procedere al cambio password su tutte le piattaforme, sia aziendali che personali, scegliendone una totalmente slegata dai propri dati personali, in maniera tale che eventuali malintenzionati in possesso dei dati all'interno del cedolino non riescano a desumere alcuna credenziale d'accesso.

Una buona password è composta da una stringa di lettere maiuscole e minuscole, numeri e caratteri speciali, che comunque deve essere di lunghezza pari o superiore agli otto caratteri. Si consiglia di utilizzare password diverse per i diversi sistemi a cui si effettua accesso, non collegate da alcun ragionamento logico tra loro: qualora ricordare tutte le diverse password risulti complicato, esistono alcune soluzioni che permettono di salvare in maniera criptata le proprie credenziali sul proprio computer/smartphone oppure in cloud; tali soluzioni vengono chiamate *"password manager"* e rappresentano un'alternativa sicura al tenere a mente le proprie password, con il chiaro rischio di scegliere password prevedibili o collegate tra loro. Alcune password manager di particolare rilievo risultano essere per es. KeePass, Zoho Vault e Dashlane che tra l'altro possono essere installati in modo gratuito.

È inoltre fortemente raccomandata l'attivazione dell'**autenticazione a due fattori** sulle principali piattaforme utilizzate, soprattutto quelle contenenti molti dati personali o critici, come gli account di accesso ad home banking e applicazioni contenenti dati sanitari, a prescindere dall'avvenuta violazione dei dati personali. L'autenticazione a due fattori è una funzione di protezione ulteriore rispetto alla password, che oggi rientra tra le *best-practice* della sicurezza sia a livello personale che aziendale in quanto non permette, con la conoscenza della sola password, di violare un account: attivando tale funzionalità verrà infatti richiesto, ad

ogni accesso, di inserire un codice inviato sul telefono cellulare o sulla casella e-mail, oppure generato da un'apposita *app*. Anche l'impronta digitale può essere utilizzata per l'autenticazione a due fattori su diverse applicazioni, se il proprio computer o il proprio *smartphone* dispone di un lettore di impronte.

Per quanto riguarda invece il rischio di *phishing* e di *spear phishing* si raccomanda di **verificare sempre**, mediante altri canali a disposizione, **l'identità dei mittenti** dei messaggi che si ricevono e sincerarsi della veridicità dell'informazione trasmessa e della richiesta, tenendo in considerazione la possibilità che ci si trovi di fronte ad un tentativo di frode, soprattutto nel caso in cui la e-mail/chiamata/pec **richieda di effettuare con urgenza azioni critiche**, come comunicare la propria password, effettuare un login, visitare un determinato link, effettuare un bonifico, trasmettere un documento identificativo. Nel caso in cui **il mittente sia ignoto** o si notino altri indirizzi e-mail sconosciuti nei campi **a/cc/ccn** (o non se ne vede neanche uno, neppure nel campo "a"), è doveroso prestare la massima attenzione poiché si tratta quasi certamente di *spam*.

Negli attacchi di *spear phishing*, il malintenzionato si firma spesso con l'identità di Fidi Nordest, di un superiore o di un collega, a volte replicando il layout della firma, per cui è necessario fare attenzione al reale indirizzo e-mail del mittente quando si ricevono messaggi che richiedono le azioni critiche sopracitate. Se il corpo dell'e-mail non risulta di agevole comprensione o se la comunicazione risulta avere un carattere non facilmente decifrabile, si suggerisce di ignorarla, in quanto a commettere errori logici, sintattici e grammaticali all'interno delle e-mail sono spesso proprio gli spammer. Sarà quindi doveroso verificare, prima di rispondere ad un'e-mail, che il destinatario sia effettivamente l'indirizzo e-mail al quale si vuole veicolare la comunicazione.

Si precisa che in nessun caso Fidi Nordest invierà via e-mail ai propri dipendenti, clienti, richieste di comunicazione della propria password, del proprio IBAN o di effettuare con urgenza azioni critiche. Qualora dovesse ricevere mail di questo tipo la preghiamo di contattare immediatamente i recapiti indicati nella FAQ "A chi posso rivolgermi per avere più informazioni relativamente all'accaduto o a questo documento?".

Cosa ha fatto Fidi Nordest per far fronte al *Data Breach*?

A seguito dell'evento occorso in data 6 luglio 2021, Fidi Nordest ha:

- subito attivato la procedura di gestione degli incidenti informatici;
- adottato l'autenticazione a due fattori per tutti la popolazione aziendale;
- revisionato e aggiornato i software utilizzati, compresi gli anti-malware;
- attivato un sistema di tracciamento delle attività dei server e della rete aziendale (cd. logging);
- notificato all'Autorità Garante per la protezione dei dati personali in data 18 luglio 2021 l'evento, indicando le informazioni disponibili in quel momento (notifica preliminare);
- incaricato una società di sicurezza esterna per un'indagine forensica dell'accaduto al fine di assicurare che l'analisi in questione venga svolta nel modo più accurato e oggettivo possibile;
- notificato nuovamente l'Autorità Garante per la protezione dei dati personali in data 4 ottobre 2021 con gli esiti dell'indagine forensica ed il supporto di professionisti esterni;
- diffidato il fornitore esterno responsabile per la sicurezza del server;
- programmato vulnerability e penetration test sulla rete aziendale; corsi aziendali sulla sicurezza e una revisione programmatica delle misure di sicurezza informatiche;

- predisposto la presente comunicazione pubblicata sul sito di Fidi Nordest e nelle bacheche aziendali per dare la massima trasparenza sul Data Breach;
- creato un canale di contatto ad hoc per eventuali dubbi, richieste o chiarimenti. è possibile indirizzare tali quesiti alla casella di posta elettronica privacy@fidinordest.it, che saranno riscontrati nei tempi consentiti dalla puntuale valutazione degli stessi.

Fidi Nordest protegge i dati degli interessati?

Ricordiamo che Fidi Nordest ha implementato un insieme di misure di sicurezza volte a proteggere il trattamento dei dati personali degli interessati, già da prima del *Data Breach*. Tra le misure di sicurezza già implementate per garantire la sicurezza del trattamento:

- **Host fisici dedicati e protetti da firewall,** allo scopo di prevenire intrusioni dall'esterno o dovute a *privilege escalation* facilitate dalla condivisione delle macchine;
- **Database su sistemi in alta affidabilità** allo scopo di mantenere la disponibilità dei dati in caso di problematiche tecniche;
- **Sistemi di autenticazione** con username e password, integrati in Active Directory al fine di garantire gestione centralizzata delle credenziali, adottando inoltre la Multi Factory Authentication (MFA) la doppia autenticazione;
- **Password** per l'autenticazione lunghe almeno 8 caratteri, contenenti lettere maiuscole e minuscole, numeri e caratteri speciali;
- **Patch management:** aggiornamento puntuale dei sistemi informatici di Fidi Nordest. Tale misura era già in essere al momento del Data Breach, ma non è stata svolta dal fornitore esterno preposto e subito diffidato a seguito dell'evento;
- **Procedura crittografata di autenticazione** verso i server dei fornitori, allo scopo di proteggere le credenziali anche quando si trovano "in transito";
- **Backup giornaliero** dei dati e definizione di un **Disaster Recovery**, al fine di garantire la disponibilità dei dati personali in caso di guasti, malfunzionamenti, incidenti o disastri naturali.

A chi posso rivolgermi per avere più informazioni relativamente all'accaduto o a questo documento?

Per qualsiasi dubbio o chiarimento sull'accaduto così come per qualsiasi questione inerente le politiche sulla protezione dei dati personali di Fidi Nordest può scrivere al Responsabile per la protezione dei dati personali (DPO) al seguente indirizzo: c.nicolin@fidinordest.it.