

## Comunicazione di violazione dei dati personali (artt. 33-34 Reg. UE 679/2016)

Gentile Interessato,  
abbiamo riscontrato che si è verificata una violazione di alcuni suoi dati personali.

Come previsto dal Reg.to UE 2016/679 – GDPR, abbiamo notificato questa violazione al Garante per la protezione dei dati personali.

### **Cosa è accaduto**

In data 9 maggio 2025, siamo venuti a conoscenza di un attacco informatico subito da un nostro fornitore, i cui dettagli – a seguito di successive e più approfondite investigazioni – ci sono stati resi noti in data 21 maggio.

Il soggetto che ha effettuato l'attacco, attraverso sofisticate tecniche informatiche e sfruttando una vulnerabilità del sistema, ha preso possesso e ha divulgato nel dark web fatture indirizzate alla clientela Arval, contenenti dati identificativi (nome, cognome e codice fiscale), dati di contatto (indirizzo) e dati bancari (IBAN) degli intestatari.

Oltre ai dati sopra indicati, alcune delle fatture in oggetto possono contenere informazioni relative al veicolo e al contratto stipulato, quali il numero di targa del veicolo noleggiato, il canone e il chilometraggio pattuiti e la durata del noleggio.

Altre fatture possono contenere la descrizione di alcuni servizi sottoscritti dal cliente, quali il servizio di rinotifica multe e il servizio di rifornimento/ricarica del veicolo. In quei casi, le fatture possono contenere dati relativi all'importo della multa, al luogo in cui è stata elevata, all'ente creditore, oppure al luogo in cui è avvenuto il rifornimento o la ricarica, oltre agli importi dei medesimi.

Purtroppo, una o più fatture della tipologia di quelle sopra descritte, la vedono come destinatario. Il periodo di emissione delle fatture relative al presente attacco è 9 ottobre 2024 – 7 dicembre 2024.

### **Cosa potrebbe significare questo per lei**

Il soggetto che ha effettuato l'attacco ha avuto accesso e divulgato dati che la riguardano, pertanto si ritiene necessario, in considerazione di quanto accaduto, trasmetterle la seguente comunicazione per indicarle anche quelli che potrebbero essere i rischi per lei connessi all'evento e le cautele che deve adottare.

In primo luogo, non possiamo escludere che chi ha effettuato l'attacco o gli eventuali 'acquirenti' dei dati dal dark web si mettano in contatto con lei e, "sfruttando" le informazioni in loro possesso, tentino di reperirne di ulteriori per poi farne un utilizzo illecito, quali ad esempio frodi e/o utilizzo della sua identità digitale.

Le raccomandiamo, quindi, di non rispondere a messaggi sospetti su social-media e di non cliccare su alcun link al loro interno, di prestare attenzione ad e-mail, SMS o messaggi telefonici e, in caso di dubbio, contattare Arval all'indirizzo

#### DATI SOCIETARI

Arval Service Lease Italia S.p.A. a socio unico - [Arval.it](https://www.arval.it)

Società soggetta all'attività di direzione e coordinamento di BNP Paribas SA

Sede legale: Via Sette Regole, 21 - 50018 Scandicci (FI)

Partita I.V.A. IT04911190488 - R.E.A. Firenze 469866 - Registro Imprese Firenze/Codice fiscale 00879960524

Capitale sociale: Euro 158.000.000 i.v.

[Azienda dotata di un Sistema di Gestione Integrato Qualità, Ambiente, Salute e Sicurezza sul Lavoro, Sicurezza Stradale, Anticorruzione](#)



[infodb@arval.it](mailto:infodb@arval.it), si da verificare l'autenticità della provenienza della richiesta.

**Misure tecniche e organizzative adottate per prevenire simili violazioni future**

Nell'immediatezza dell'attacco il fornitore ha provveduto ad adottare delle misure tecniche al fine di ulteriormente rafforzare la propria sicurezza, quali:

- applicazione della patch di sicurezza alla vulnerabilità del sistema individuata (CVE-2024-55956);
- implementazione delle firme su modulo IPS (Inclusion Prevention System), in modo da intercettare e prevenire ulteriori attacchi che sfruttino la medesima vulnerabilità;
- implementazione regola di detection puntuale relativa alla vulnerabilità;
- impedimento di successivi illegittimi accessi tramite inclusione nella black list del firewall degli indirizzi IP sorgenti dei soggetti che hanno effettuato l'attacco;
- reset di tutte le password di amministratore di sistema.

Al contempo, Arval sta effettuando ulteriori verifiche tecniche sul fornitore, per l'adozione da parte di quest'ultimo di misure addizionali, in modo da evitare o limitare il più possibile in futuro simili accadimenti.

Tali misure consistono in:

- implementazione di un monitoraggio specifico dell'infrastruttura con invio dei log in tempo reale al SIEM (Security Information and Event Management);
- monitoraggio del traffico di rete al fine di permettere al sistema di threat intelligence di individuare eventuali anomalie nella quantità di dati in uscita;
- implementazione di misure di sicurezza per aumentare il livello di segregazione delle macchine virtuali che ospitano software di terze parti, in modo da evitare contaminazioni.

Arval sta, altresì, valutando le informazioni ad oggi contenute nelle fatture, al fine di individuare eventuali dati non strettamente indispensabili, cioè che potrebbero essere dalle stesse eliminati senza pregiudizio per la trasparenza verso la propria clientela e l'efficienza, si da minimizzare l'impatto per il futuro di simili casi.

Arval, infine, si impegna al monitoraggio dei reclami provenienti dalla fascia di clienti nel perimetro dell'attacco, in modo da intercettare ed eventualmente prevenire frodi o truffe ai danni degli interessati.

Nello scusarci per quanto accaduto, rimaniamo a disposizione per qualsiasi supporto, informazione e chiarimento; a tale scopo potrà contattare la seguente casella mail: [infodb@arval.it](mailto:infodb@arval.it)

Cordiali Saluti,

**Arval Service Lease Italia S.p.A.**

**Il Direttore Generale**

**Dario Casiraghi**

DATI SOCIETARI

Arval Service Lease Italia S.p.A. a socio unico - [Arval.it](https://www.arval.it)

Società soggetta all'attività di direzione e coordinamento di BNP Paribas SA

Sede legale: Via Sette Regole, 21 - 50018 Scandicci (FI)

Partita I.V.A. IT0491190488 - R.E.A. Firenze 469866 - Registro Imprese Firenze/Codice fiscale 00879960524

Capitale sociale: Euro 158.000.000 i.v.

[Azienda dotata di un Sistema di Gestione Integrato Qualità, Ambiente, Salute e Sicurezza sul Lavoro, Sicurezza Stradale, Anticorruzione](#)