GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

DIPARTIMENTO TECNOLOGIE DIGITALI
E SICUREZZA INFORMATICA

Punto di accesso telematico ai servizi della pubblica amministrazione di cui all'art. 64-*bis* del CAD

(fascicolo n. 165057)

Relazione tecnica sulle interazioni dell'App IO con i servizi di Google, Mixpanel e Instabug

Piazza Venezia 11 - 00187 Roma
Tel. +39 06 696771
PEC: protocollo@pec.gpdp.it
www.gpdp.it

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

SOMMARIO

1. PREMESSA

Preliminarmente, si evidenzia che le considerazioni di seguito riportate sono effettuate a seguito dell'analisi tecnica dell'App IO nella sua versione 1.24.0.6 per dispositivi con sistema operativo Android. Tuttavia, alcune di esse sono verosimilmente riferibili anche all'App IO per dispositivi con sistema operativo iOS.

In un primo momento, è stato analizzato il contenuto del *file* "AndroidManifest.xml" che, tra le altre cose, indica le componenti, fornite anche da terze parti, utilizzate da un'app per dispositivi Android, constatando all'interno dell'App IO (versione 1.24.0.6) la presenza di elementi relativi a servizi forniti dalle società Google LLC (di seguito "Google"), Mixpanel Inc. (di seguito "Mixpanel") e Instabug Inc. (di seguito "Instabug").

Nei seguenti paragrafi sono descritte e analizzate le interazioni dell'App IO con i servizi forniti delle predette società.

2. LE INTERAZIONI CON I SISTEMI DI GOOGLE

Dall'analisi del traffico generato nel corso delle attività di analisi dinamica effettuate il 4 maggio 2021, è stato verificato che l'App IO interagisce con alcuni sistemi riconducibili a Google. In particolare, è stata constatata la presenza di connessioni a servizi o risorse individuati tramite i seguenti indirizzi in notazione URL:

1. "https://firebaseinstallations.googleapis.com/v1/projects/io-app-41dc2/installations";
2. "https://app-measurement.com/config/app/1:260468725946:android:965f19069c173eea4d0a83";
3. "https://app-measurement.com/a";
4. "https://fonts.googleapis.com/css2";
5. "https://fonts.gstatic.com/s/titilliumweb/v9/NaPecZTIAOhVxoMyOr9n_E7fdMPmDaZRbrw.woff2";
6. "https://fonts.gstatic.com/s/titilliumweb/v9/NaPDcZTIAOhVxoMyOr9n_E7ffHjDGItzY5abuWI.woff2".

2.1. L'ubicazione dei sistemi di Google

Allo scopo di determinare l'ubicazione dei sistemi informatici a cui sono inviati i predetti dati, sono state effettuate alcune interrogazione tecniche di tipo *nslookup* e *whois* (cfr. all. 1 al verbale delle operazioni compiute del 27 maggio 2021), da cui è emerso che:

- al nome di dominio "firebaseinstallations.googleapis.com" sono associati i seguenti indirizzi IP:
  - 142.250.180.138, assegnato a Google LLC (AS15169);
  - 2a00:1450:4002:400::200a, assegnato a Google LLC (AS15169);
- al nome di dominio "app-measurement.com" sono associati i seguenti indirizzi IP:
  - 216.58.208.142, assegnato a Google LLC (AS15169);
  - 2a00:1450:4002:805::200e, assegnato a Google LLC (AS15169);
- al nome di dominio "fonts.googleapis.com" sono associati i seguenti indirizzi IP:
  - 142.250.184.74, assegnato a Google LLC (AS15169);
  - 2a00:1450:4002:405::200a, assegnato a Google LLC (AS15169);
- il nome di dominio "fonts.gstatic.com" è un *alias* (CNAME) del nome di dominio "gstaticadssl.l.google.com", al quale sono associati i seguenti indirizzi IP:
  - 142.250.184.35, assegnato a Google LLC (AS15169);
  - 2a00:1450:4002:404::2003, assegnato a Google LLC (AS15169).

Gli indirizzi IP sopra riportati, pur apparendo riferibili a sistemi informatici ubicati negli Stati Uniti, sono indirizzi IP di tipo *anycast* – utilizzati da Google per effettuare il bilanciamento del carico – per i quali, senza ulteriori informazioni, non è possibile risalire alla possibile ubicazione dei relativi sistemi informatici. Tuttavia, sulla base di quanto rappresentato da Google (cfr. all. 5 e 7 al verbale

delle operazioni compiute del 27 maggio 2021), l'utilizzo dei predetti servizi di Google può comportare la raccolta, il trattamento e la conservazione dei dati su sistemi ubicati negli Stati Uniti.

2.2. I dati inviati a Google

Con riferimento al primo URL ("https://firebaseinstallations.googleapis.com/v1/projects/io-app-41dc2/installations"), è stata registrata dal "Mobile Security Framework" una richiesta HTTP (*hypertext transfer protocol*) di tipo POST con i seguenti parametri in formato JSON:

- "fid", con valore "eeUNuclwQjOL_RN9ztHmx0" che rappresentata un identificativo univoco dell'installazione dell'app su uno specifico dispositivo;
- "appId", con valore "1:260468725946:android:965f19069c173eea4d0a83", che rappresenta l'identificativo dell'App IO, che include al suo interno l'identificativo "260468725946"; memorizzato nella variabile "GCM_SENDER_ID" presente nel file "it/pagopa/io/app/BuildConfig.java";
- "authVersion", con valore "FIS_v2";
- "sdkVersion", con valore "a:16.3.5".

La predetta richiesta contiene, tra gli altri, l'*header* HTTP denominato "x-goog-api-key" con valore "AIzaSyAnMZ-gF4jeRva9UibHnq9o0MGWbpcy3K0", che rappresenta la chiave associata da Google all'App IO, memorizzata nella variabile "google_api_key" presente nel codice sorgente dell'app.

In particolare, è stato constatato che, al suo primo avvio su un dispositivo Android, l'App IO effettua in modo automatico l'inizializzazione dei servizi Firebase di Google, creando un identificativo univoco associato all'installazione dell'App IO (c.d. "fid") e interagendo con i sistemi di Google per l'invio di tale identificativo e la ricezione di alcuni dati di configurazione.

In particolare, all'interno del codice sorgente dell'App IO sono state trovare tracce di codice relative ai servizi "Firebase Cloud Messaging" ("FCM", che consente di inviare notifiche *push* ai dispositivi degli utenti) e "Firebase Analytics" ("FA", che consente di monitorare l'utilizzo dell'app da parte degli utenti, raccogliendo dati degli eventi *in-app*).

Con riferimento al secondo URL ("https://app-measurement.com/config/app/1:260468725946:android:965f19069c173eea4d0a83"), sono state registrate dal "Mobile Security Framework" due richieste HTTP di tipo GET con i seguenti parametri:

- "app_instance_id", con valore "e8e1da927ae02d13dc142921983c3ac2" che rappresentata un identificativo univoco dell'installazione dell'app su uno specifico dispositivo;
- "platform", con valore "android";
- "gmp_version", con valore "25001".

Con riferimento al terzo URL ("https://app-measurement.com/a"), sono state registrate dal "Mobile Security Framework" due richieste HTTP di tipo POST con l'invio, in formato binario, di alcune informazioni relative al dispositivo dell'utente e all'installazione dell'App IO.

Con riferimento al quarto URL ("https://fonts.googleapis.com/css2"), al quinto URL ("https://fonts.gstatic.com/s/titilliumweb/v9/NaPecZTIAOhVxoMyOr9n_E7fdMPmDaZRbrw.woff2") e al sesto URL ("https://fonts.gstatic.com/s/titilliumweb/v9/NaPDcZTIAOhVxoMyOr9n_E7ffHjDGItzY5abuWI.woff2"), sono state registrate dal "Mobile Security Framework" tre distinte richieste HTTP di tipo GET, generate all'atto della consultazione sella sezione dell'App IO relativa ai servizi erogati da enti locali (*referer* "https://io.italia.it/app-content/enti-servizi.html"), volte ad effettuare il download dei *font* tipografici utilizzati in quella sezione dell'App IO.

2.3. Ulteriori considerazioni sull'utilizzo dei servizi di Google

Infine, sempre attraverso l'analisi del codice sorgente dell'App IO, sono constatate le modalità con le quali sono state configurate alcune funzionalità messe a disposizione da Google.

In particolare, Google mette a disposizione degli sviluppatori apposite funzionalità per attivare/disattivare la generazione automatica degli identificativi sopra citati e la raccolta dei dati dai dispositivi degli utenti e per gestire il conferimento e la revoca del consenso da parte degli utenti all'invio di tali dati (cfr. all. 6 al verbale delle operazioni compiute del 27 maggio 2021).

Anche se le librerie FCM e FA di Google, per impostazione predefinita, sono programmate per generare un identificativo univoco per l'app nella quale sono richiamate, utilizzato per la ricezione di notifiche *push* o per l'invio di dati relativi a eventi oggetto di tracciamento, le predette funzionalità consentono agli sviluppatori di un'app di modificare, a seconda delle esigenze, le modalità di funzionamento delle librerie FCM e FA di Google disabilitando l'inizializzazione automatica dei predetti servizi Firebase e consentendo di attivare tali servizi solo per quegli utenti che hanno prestato il loro consenso all'archiviazione di informazioni sul proprio dispositivo e all'accesso alle informazioni già archiviate. In ogni caso, Google mette a disposizione degli sviluppatori altre funzionalità per consentire una gestione del conferimento e della revoca del consenso di ciascun utente sulla base delle scelte effettuate dallo stesso all'interno dell'app installata sul proprio dispositivo.

Nel caso in esame, l'App IO risulta essere configurata per generare automaticamente l'identificativo univoco dell'installazione dell'app (per la ricezione di notifiche *push* o per l'invio di dati relativi a eventi oggetto di tracciamento) senza che l'utente possa modificare tale impostazione predefinita.

Infine, sono emersi alcuni elementi di criticità anche in relazione alle modalità con cui l'App IO utilizza *font* tipografici ("stili di carattere") esterni, forniti da Google.

In particolare, è stato constatato che la consultazione della sezione relativa ai servizi degli enti locali comporta la trasmissione a Google di alcuni dati di navigazione – quali l'indirizzo IP, l'orario di connessione e altri parametri relativi al sistema operativo e al tipo di terminale – degli utenti dell'App IO, non necessaria in termini funzionali e dunque eccedente. Ciò, senza che l'utente venga adeguatamente informato di tale circostanza.

Al riguardo, si evidenzia che sarebbe stato possibile configurare l'App IO, mantenendone invariate le caratteristiche grafiche e funzionali, in modo da evitare il conferimento a fornitori esterni di dati riferibili ai suoi utenti, incorporando i *font* tipografici utilizzati all'interno dell'app.

3. LE INTERAZIONI CON I SISTEMI DI MIXPANEL

Dall'analisi del traffico generato nel corso delle attività di analisi dinamica effettuate il 4 maggio 2021, è stato verificato che l'App IO interagisce con alcuni sistemi riconducibili a Mixpanel. In particolare, è stata constatata la presenza di numerose connessioni ai seguenti URL:

1. "https://decide.mixpanel.com/decide";
2. "https://api-eu.mixpanel.com/track".

3.1. L'ubicazione dei sistemi di Mixpanel

Allo scopo di individuare l'ubicazione dei sistemi informatici a cui sono invitati i predetti dati, sono state effettuate alcune interrogazione tecniche di tipo *nslookup* e *whois* (cfr. all. 1 al verbale delle operazioni compiute del 27 maggio 2021), da cui è emerso che:

- il nome di dominio "decide.mixpanel.com" è un *alias* (CNAME) del nome di dominio "api.mixpanel.com", al quale sono associati i seguenti indirizzi IP:
  - 35.190.25.25, assegnato a Google LLC (AS15169);
  - 35.186.241.51, assegnato a Google LLC (AS15169);
  - 107.178.240.159, assegnato a Google LLC (AS15169);
  - 130.211.34.183, assegnato a Google LLC (AS15169);

- al nome di dominio "api-eu.mixpanel.com" è associato il seguente indirizzo IP:
  - 34.96.125.79, assegnato a Google LLC (AS15169).

Gli esiti delle predette analisi tecniche risultano coerenti con quanto emerge dalla documentazione agli atti (cfr. all. D.05 alla relazione di servizio del 27 maggio 2021), secondo la quale Mixpanel si avvale di risorse elaborative e di *storage* fornite da Google. Gli indirizzi IP sopra riportati, pur apparendo riferibili a sistemi informatici ubicati negli Stati Uniti, sono indirizzi IP di tipo *anycast* – utilizzati da Google per effettuare il bilanciamento del carico – per i quali, senza ulteriori informazioni, non è possibile risalire alla possibile ubicazione dei relativi sistemi informatici. Tuttavia, sulla base di quanto rappresentato da Mixpanel (cfr. all. 10 e 11 al verbale delle operazioni compiute del 27 maggio 2021), l'utilizzo del nome di dominio "api.mixpanel.com" comporta la raccolta, il trattamento e la conservazione dei dati su sistemi ubicati negli Stati Uniti, mentre l'utilizzo del nome di dominio "api-eu.mixpanel.com" comporta la raccolta, il trattamento e la conservazione dei dati su sistemi ubicati nell'Unione europea, fermo restando che l'accesso remoto a tali sistemi di trattamento da parte di un soggetto stabilito al di fuori dell'Unione europea configura comunque un trasferimento di dati verso Paesi terzi.

3.2. I dati inviati a Mixpanel

Con riferimento al primo URL ("https://decide.mixpanel.com/decide"), sono state registrate dal "Mobile Security Framework" diverse richieste HTTP (*hypertext transfer protocol*) di tipo GET con i seguenti parametri:

- "version", con valore "1";
- "lib", con valore "android";
- "token", con valore "0cb505dace6f4b3ceb9e17c7fcd7c66f", che rappresenta il "Project Token" associato da Mixpanel all'App IO, memorizzato nella variabile "MIXPANEL_TOKEN" presente nel file "it/pagopa/io/app/BuildConfig.java";
- "distinct_id", che rappresentata un identificativo univoco dell'utente che sta utilizzando l'App IO (in assenza dell'identificativo dell'utente, è pari al valore dell'identificativo del dispositivo utilizzato);
- "properties", che contiene, in formato JSON, le seguenti informazioni:
  - "$android_lib_version", con valore "5.6.8", che indica la versione della libreria Mixpanel utilizzata;
  - "$android_app_version", con valore "1.24.0.6", e "$android_app_release", con valore "10078640", che indicano la versione dell'App IO utilizzata;
  - "$android_version", con valore "8.0.0", e "$android_device_model", con valore "Genymotion+'Phone'+version", che indicano la versione del sistema operativo e il modello del dispositivo utilizzato.

Con riferimento invece al secondo URL ("https://api-eu.mixpanel.com/track"), sono state registrate diverse richieste HTTP (*hypertext transfer protocol*) di tipo POST con il parametro "data" che contiene, con codifica Base64 e in formato JSON, le seguenti informazioni:

- "event", che identifica l'evento oggetto di tracciamento;
- "properties", che contiene, tra le altre, le seguenti informazioni:
  - "mp_lib" e "$lib_version", che indicano la versione della libreria Mixpanel utilizzata;
  - "$os", "$os_version", "$manufacturer", "$brand", "$model", "$google_play_services", "$screen_dpi", "$screen_height", "$screen_width", "$has_nfc", "$has_telephone", "$carrier", "$wifi" e "$bluetooth_version", che costituiscono informazioni sul dispositivo utilizzato e sul suo sistema operativo;
  - "$app_version", "$app_version_string", "$app_release" e "$app_build_number", che indicano la versione dell'App IO utilizzata;

- "token", con valore "0cb505dace6f4b3ceb9e17c7fcd7c66f", che rappresenta il "Project Token" associato da Mixpanel all'App IO;
- "time", che rappresenta la data e l'ora dell'evento nella notazione Unix;
- "$device_id", con valore "d403a0e6-a644-4de3-b8b5-61be845af512", che rappresentata l'identificativo del dispositivo utilizzato;
- "$user_id", con valore " O M I S S I S ", che rappresentata l'identificativo dell'utente che sta utilizzando l'App IO;
- "distinct_id", che rappresentata un identificativo univoco dell'utente che sta utilizzando l'App IO (assume lo stesso valore di "$user_id" o, in sua assenza, di "$device_id");

– "$mp_metadata", che contiene le seguenti informazioni:
- "$mp_event_id", che rappresenta il codice identificativo dell'evento;
- "$mp_session_id", che rappresenta il codice identificativo della sessione utente;
- "$mp_session_seq_id", che rappresenta l'identificativo sequenziale dell'evento all'interno della sessione utente;
- "$mp_session_start_sec", che rappresenta il *timestamp* di avvio della sessione utente.

Dall'analisi del codice sorgente dell'App IO e del traffico generato verso i sistemi Mixpanel (cfr. all. 2 al verbale delle operazioni compiute del 27 maggio 2021) è stato verificato che l'App IO è configurata per inviare alcune informazioni a Mixpanel in occasione di determinate azioni effettuate da un utente all'interno dell'app. I principali eventi che risultano essere oggetto di tracciamento, di cui è stata verificata l'esistenza, sono indicati nella tabella in allegato 1.

Al riguardo, si evidenzia che tra i diversi eventi oggetto di tracciamento risultano presenti anche eventi relativi ad alcuni specifici servizi resi disponibili attraverso l'App IO:

a) bonus vacanze di cui all'art. 176 del d.l. n. 34/2020, tra i quali gli eventi relativi alla verifica dei requisiti per la richiesta del bonus e alla sua generazione (dei quali tuttavia non è stato possibile acquisire ulteriori elementi nel corso delle attività di analisi dinamica dell'App IO);

b) programma *cashback* di cui all'art. 1, commi da 288 a 290, della l. n. 160/2019, tra i quali:

   1) evento "BPD_TRANSACTIONS_SUCCESS", comprensivo dell'elenco delle transazioni che partecipano al programma *cashback* con l'indicazione del periodo di partecipazione, degli identificativi della transazione (idTrxAcquirer e idTrxIssuer), dell'identificativo e del circuito dello strumento di pagamento elettronico (hashPan e circuitType) e della data/ora della transazione (trxDate);

   2) evento "BPD_PAYMENT_METHOD_ACTIVATION_SUCCESS", comprensivo dell'elenco degli strumenti di pagamento elettronico dell'utente con l'indicazione dell'identificativo della carta (hashPan), dello stato di adesione al programma *cashback* (activationStatus), della data/ora di adesione (activationDate) e della data/ora di revoca dell'adesione (deactivationDate);

c) piattaforma PagoPA di cui all'art. 5, comma 2, del d.lgs. n. 82/2005, tra i quali gli eventi relativi all'aggiunta di strumenti di pagamento al portafoglio dell'utente e all'esecuzione di pagamenti a favore di pubbliche amministrazioni e gestori di pubblici servizi (dei quali tuttavia non è stato possibile acquisire ulteriori elementi nel corso delle attività di analisi dinamica dell'App IO).

Le librerie di tracciamento di Mixpanel inviano i dati, relativi a ciascun evento oggetto di tracciamento, in associazione a un identificativo univoco denominato "distinct_id". Dall'analisi del codice sorgente dell'App IO e del traffico generato verso i sistemi Mixpanel, è stato verificato che a ciascun utente dell'App IO è associato un identificativo univoco che è generato applicando al suo codice fiscale una funzione di *hashing* (funzione SHA-256).

3.3. Ulteriori considerazioni sull'utilizzo delle librerie di Mixpanel

Infine, sempre attraverso l'analisi del codice sorgente dell'App IO, sono constatate le modalità con le quali sono state configurate alcune funzionalità offerte da Mixpanel (cfr. all. 9, 12 e 13 al verbale delle operazioni compiute del 27 maggio 2021):

- *Geolocation Tracking*: Mixpanel, per impostazione predefinita, associa ai dati raccolti alcune informazioni relative all'ubicazione degli utenti di un'app (città, regione, Stato); tali informazioni sono ricavate a partire dagli indirizzi IP degli utenti (che, secondo quanto riportato da Mixpanel, sarebbero cancellati dopo tale elaborazione) mediante un servizio di una terza parte (MaxMind Inc. con sede negli Stati Uniti, di cui non è possibile escludere un'eventuale coinvolgimento nel trattamento degli indirizzi IP degli utenti); Mixpanel consente agli sviluppatori di disattivare tale funzionalità mediante un'apposita configurazione dell'app da inserire, nel caso di dispositivi Android, nel file "AndroidManifest.xml"; nel caso in esame, risulta che per l'App IO la funzionalità di "*geolocation tracking*" sia attivata;
- *Opt-Out Users*: Mixpanel mette a disposizione degli sviluppatori apposite funzionalità per attivare/disattivare la raccolta dei dati dai dispositivi degli utenti e per gestire il conferimento e la revoca del consenso da parte degli utenti all'invio di tali dati; anche se le librerie di Mixpanel, *by default*, sono programmate per inviare i dati relativi a tutti gli eventi oggetto di tracciamento, le predette funzionalità consentono agli sviluppatori di un'app di modificare, a seconda delle esigenze, le modalità di funzionamento delle librerie di tracciamento configurando, come "stato" predefinito degli utenti dell'app, lo "stato *opt-out*" in modo che l'accesso ai dati archiviati sui dispositivi avvenga solo per quegli utenti che hanno esplicitamente prestato il consenso; in ogni caso, Mixpanel mette a disposizione degli sviluppatori altre funzionalità per consentire una gestione puntuale dello "stato" di ciascun utente ("*opt-out*" o "*opt-in*") sulla base delle scelte effettuate dallo stesso all'interno dell'app installata sul proprio dispositivo; nel caso in esame, l'App IO risulta essere configurata per inviare a Mixpanel i dati relativi a tutti gli eventi oggetto di tracciamento di ciascun utente senza che quest'ultimo possa modificare tale impostazione predefinita;
- *Randomly Generated Identifiers:* Mixpanel mette a disposizione degli sviluppatori alcune funzionalità che consentono di generare, in modo pseudocasuale, l'identificativo univoco (distinct_id) di ciascun utente dell'App IO; nel caso in esame, l'App IO risulta configurata in modo da non avvalersi di tale possibilità e da generare gli identificativi univoci degli utenti con una funzione deterministica che a partire dal codice fiscale di un utente produce sempre lo stesso risultato anche in caso di utilizzo di un diverso dispositivo mobile;
- *Server-Side Implementation*: Mixpanel rende disponibile la documentazione di tutte le proprie API, consentendo agli sviluppatori di raccogliere i dati anche senza fare ricorso alle librerie di tracciamento per dispositivi Android e iOS; tale documentazione consente agli sviluppatori di progettare un'app in modo da raccogliere i dati relativi agli eventi oggetto di tracciamento su un proprio *server* e successivamente inviarli a Mixpanel utilizzando le predette API, avendo in tal modo un maggior controllo dei dati inviati; nel caso in esame, tale possibilità non risulta essere stata presa in considerazione per l'App IO che è configurata per inviare i dati relativi agli eventi oggetto di tracciamento direttamente ai sistemi di Mixpanel.

4. LE INTERAZIONI CON I SISTEMI DI INSTABUG

Dall'analisi del traffico generato nel corso delle attività di analisi dinamica effettuate il 4 maggio 2021, è stato verificato che l'App IO interagisce anche con alcuni sistemi riconducibili a Instabug. In particolare, è stata constatata la presenza di connessioni ai seguenti URL:

1) "https://api.instabug.com/api/sdk/v3/features";

2) "https://api.instabug.com/api/sdk/v3/first_seen";
3) "https://api.instabug.com/api/sdk/v3/surveys/v7";
4) "https://api.instabug.com/api/sdk/v3/application_categories";
5) "https://api.instabug.com/api/sdk/v3/chats/sync".

4.1. L'ubicazione dei sistemi di Instabug

Allo scopo di individuare l'ubicazione dei sistemi informatici a cui sono invitati i predetti dati, sono state effettuate alcune interrogazione tecniche di tipo *nslookup* e *whois* (cfr. all. 1 al verbale delle operazioni compiute del 27 maggio 2021), da cui è emerso che al nome di dominio "api.instabug.com" sono associati i seguenti indirizzi IP:

- 3.214.89.159, assegnato ad Amazon Technologies Inc. (AS14618);
- 52.4.224.84, assegnato ad Amazon Technologies Inc. (AS14618);
- 52.205.135.59, assegnato ad Amazon Technologies Inc. (AS14618);
- 34.194.144.112, assegnato ad Amazon Technologies Inc. (AS14618);
- 34.225.41.153, assegnato ad Amazon Technologies Inc. (AS14618);
- 54.157.66.209, assegnato ad Amazon Technologies Inc. (AS14618);
- 3.208.228.239, assegnato ad Amazon Technologies Inc. (AS14618);
- 3.218.11.141, assegnato ad Amazon Technologies Inc. (AS14618).

Gli esiti delle predette analisi tecniche risultano coerenti con quanto emerge dalla documentazione agli atti (cfr. all. 15 al verbale delle operazioni compiute del 27 maggio 2021), secondo la quale Instabug si avvale di risorse elaborative e di *storage* fornite da Amazon Web Services, Inc. (di seguito "Amazon Web Services"). Gli indirizzi IP sopra riportati appaiono riferibili a sistemi informatici ubicati negli Stati Uniti.

4.2. I dati inviati a Instabug

Con riferimento al primo URL ("https://api.instabug.com/api/sdk/v3/features"), è stata registrata una richiesta HTTP di tipo GET con i seguenti parametri:

- "application_token" con valore "5c2d0f12fa12f9afc535585e5b7a9e79" che rappresenta il *token* associato da Instabug all'App IO, memorizzato nella variabile "INSTABUG_TOKEN" presente nel file "it/pagopa/io/app/BuildConfig.java";
- "uuid", con valore "94f26669-f0e3-42d7-84b6-725ea4094155" che rappresentata un identificativo univoco dell'utente.

Dall'analisi del codice sorgente dell'App IO e della configurazione delle librerie di Instabug (cfr. all. 3 al verbale delle operazioni compiute del 27 maggio 2021) è stato verificato che nel corso di tale interazione l'App IO riceve i parametri di configurazione delle librerie di Instabug. In particolare, è stato constatato che l'App IO è configurata per consentire agli utenti di inviare segnalazioni (c.d. *bug reporting*) e per inviare automaticamente alcune informazioni in caso di malfunzionamenti dell'app (c.d. *crash reporting*).

Con riguardo alla funzionalità di *bug reporting*, è stato constatato che la stessa viene resa disponibile agli utenti dell'App IO all'interno dell'area "IO ti aiuto" presente in ogni sezione dell'app e che la stessa può essere utilizzata per segnalare "*eventuali problemi dell'app*" o per inviare "*suggerimenti* […] *relativi a migliorie o nuove funzionalità*". All'atto dell'invio di una segnalazione, l'utente può decidere se associare o meno il proprio codice fiscale alla segnalazione "*in modo da rendere più semplice la risoluzione del problema*". Dopo aver selezionato l'ambito della segnalazione (Cashback, Accesso tramite SPID, Accesso tramite CIE, Bonus Vacanze, Pagamento PagoPA), l'utente viene invitato a "*non inserire dati sensibili nelle* […] *segnalazioni*" e a "*includere un elenco di passaggi per riprodurre il problema*". L'App IO è configurata per inviare a Instabug delle seguenti informazioni:

a) *User Attributes*, che comprendono la versione dell'App IO, il tipo e l'ubicazione del dispositivo utilizzato, la versione del sistema operativo, la durata della sessione utente, unitamente a altre informazioni (versione del *backend*, schermata attiva, gestore dell'identità utilizzato, identificativo dell'ultimo messaggio visualizzato, *support token*);

b) *Bug Report Fields*, che comprendono l'indirizzo e-mail (inserito facoltativamente dall'utente) e il testo della segnalazione;

c) *Attachments*, che possono essere immagini o video che l'utente intende allegare alla segnalazione;

d) *Logs*, che comprendono *Console Logs*, *Instabug Logs*, *User Steps*, *Repro Steps* e *User Events* (cfr. all. 17, 18, 19 e 20 al verbale delle operazioni compiute del 27 maggio 2021);

e) *Repros Steps*, che includono l'elenco delle ultime azioni effettuati dall'utente precedentemente all'evento di *crash*;

f) *Session Profiler*, che comprende informazioni sul dispositivo nei 60 secondi precedenti all'invio del *report* di crash (CPU, RAM, memoria, connettività di rete, batteria, orientamento verticale/orizzontale del dispositivo);

g) *View Hierarchy*, che include informazioni sull'interfaccia utente dell'app (componenti grafiche e relative proprietà).

Con riguardo invece alla funzionalità di *crash reporting*, è stato constatato che le librerie di Instabug sono configurate per archiviare nel terminale dell'utente dell'App IO diverse tipologie di informazioni (*User Attributes*, *Repros Steps*, *Session Profiler*, *Logs*). Allo stato non è chiaro se tali informazioni vengono accedute e inviate automaticamente a Instabug al verificarsi di un evento di *crash* dell'App IO (che non è stato possibile riprodurre nel corso delle attività di analisi dinamica di tale app).

Con riferimento al secondo URL ("https://api.instabug.com/api/sdk/v3/first_seen"), è stata registrata una richiesta HTTP di tipo GET con i seguenti parametri:

- "application_token" con valore "5c2d0f12fa12f9afc535585e5b7a9e79" che rappresenta il *token* associato da Instabug all'App IO, memorizzato nella variabile "INSTABUG_TOKEN" presente nel file "it/pagopa/io/app/BuildConfig.java";
- "uuid", con valore "94f26669-f0e3-42d7-84b6-725ea4094155" che rappresentata un identificativo univoco dell'utente.

Con riferimento al terzo URL ("https://api.instabug.com/api/sdk/v3/surveys/v7"), è stata registrata una richiesta HTTP di tipo GET con i seguenti parametri:

- "application_token" con valore "5c2d0f12fa12f9afc535585e5b7a9e79" che rappresenta il *token* associato da Instabug all'App IO, memorizzato nella variabile "INSTABUG_TOKEN" presente nel file "it/pagopa/io/app/BuildConfig.java";
- "uuid", con valore "94f26669-f0e3-42d7-84b6-725ea4094155" che rappresentata un identificativo univoco dell'utente;
- "locale", con valore "it".

Con riferimento al quarto URL ("https://api.instabug.com/api/sdk/v3/application_categories"), è stata registrata una richiesta HTTP di tipo GET con i seguenti parametri:

- "application_token" con valore "5c2d0f12fa12f9afc535585e5b7a9e79" che rappresenta il *token* associato da Instabug all'App IO, memorizzato nella variabile "INSTABUG_TOKEN" presente nel file "it/pagopa/io/app/BuildConfig.java".

Con riferimento al quinto URL ("https://api.instabug.com/api/sdk/v3/chats/sync"), è stata registrata una richiesta HTTP di tipo POST con i seguenti parametri in formato JSON:

- "application_token" con valore "5c2d0f12fa12f9afc535585e5b7a9e79" che rappresenta il *token* associato da Instabug all'App IO, memorizzato nella variabile "INSTABUG_TOKEN" presente nel file "it/pagopa/io/app/BuildConfig.java";
- "uuid", con valore "94f26669-f0e3-42d7-84b6-725ea4094155" che rappresentata un identificativo univoco dell'utente;
- "messages_count", con valore "0".

4.3. Ulteriori considerazioni sull'utilizzo delle librerie di Instabug

Instabug mette a disposizione degli sviluppatori la possibilità di ospitare il *backend* di Instabug sulla propria infrastruttura IT (c.d. *On-Premise Hosting*) o su un *cloud* privato (c.d. *Dedicated Hosting*). Nel caso in esame, tale possibilità non risulta essere stata presa in considerazione per l'App IO che è configurata per inviare i dati relativi agli eventi oggetto di tracciamento direttamente ai sistemi di Instabug.

5. LE VALUTAZIONI DI QUESTO DIPARTIMENTO

5.1. Sull'archiviazione di informazioni nel terminale dell'utente e sull'accesso alle informazioni archiviate

Dalla documentazione in atti e dalle analisi svolte è emerso che l'App IO, all'atto del primo avvio e durante la sua esecuzione sul dispositivo di un utente, archivia talune informazioni sullo stesso e, in alcuni casi, accede a informazioni ivi già archiviate per trasmetterle a Google, Mixpanel e Instabug (cfr. paragrafi 2, 3 e 4).

Secondo quanto riportato da PagoPA nell'informativa resa agli utenti (cfr. all. I alla relazione di servizio del 27 maggio 2021), tali informazioni sono raccolte e trattate per finalità di "*assistenza, debug e miglioramento dell'App IO*". In particolare, PagoPA rappresenta che i "*dati sono raccolti tramite sistemi di fornitori terzi nominati responsabili del trattamento, e utilizzati esclusivamente per finalità di assistenza tecnica (dietro* […] *richiesta) e al fine elaborare statistiche sul funzionamento dei* […] *sistemi, e mediante l'adozione di meccanismi di pseudonimizzazione*". Inoltre, nella stessa informativa, viene evidenziato come PagoPA possa "*procedere all'anonimizzazione e aggregazione di dati relativi alla navigazione allo scopo di migliorare il funzionamento dell'App*".

Inoltre, nella valutazione di impatto sulla protezione dei dati sui trattamenti relativi all'App IO (versione del 26 giugno 2020), PagoPA rappresenta che i dati raccolti mediante gli strumenti di tracciamento forniti da Mixpanel e Instabug sono utilizzati per:

O M I S S I S

O M I S S I S

Infine, nella valutazione di impatto sulla protezione dei dati relativa ai trattamenti effettuati nell'ambito del programma *cashback* (versione del 24 novembre 2020), svolta dal Ministero dell'economia e delle finanze con il supporto di PagoPA, è rappresentato che

O M I S S I S

Tuttavia, sulla base delle analisi svolte, è stato constatato che l'utilizzo delle librerie *software* di Google, Mixpanel e Instabug presenti all'interno dell'App IO (descritte nei paragrafi 2, 3 e 4) determina, a tutti gli effetti, effetti di tracciamento in grado di ricondurre a soggetti determinati, identificati o identificabili, specifiche azioni o schemi comportamentali ricorrenti nell'uso dei diversi servizi offerti all'interno dell'App IO.

Con riferimento all'utilizzo delle librerie di Google, è emerso che l'App IO, al suo primo avvio su un dispositivo Android, effettua in modo automatico l'inizializzazione dei servizi Firebase di Google, creando un identificativo univoco associato all'installazione dell'app (c.d. "fid"), utilizzato per l'interazione con i sistemi di Google. Tale identificativo, pur risultando necessario per l'invio di notifiche *push*, viene generato, per impostazione predefinita, in relazione ai dispositivi di tutti gli utenti dell'App IO a prescindere dalla volontà di ciascuno di attivare tale canale di comunicazione.

Inoltre, diversamente da quanto rappresentato da PagoPA, sono state rinvenute nel codice sorgente, e rilevate nel traffico generato nel corso delle attività di analisi dinamica, alcune interazioni dell'App IO con i servizi Firebase Analytics di Google che consentono quantomeno di monitorare le installazioni dell'App IO sui dispositivi degli utenti. Ciò, senza che sia chiara la

finalità di tale trattamento e senza che l'utente sia adeguatamente informato di tale circostanza o che possa esprimere il proprio consenso previsto dall'art. 122 del Codice.

Con riguardo, invece, al ricorso a Mixpanel, si osserva che lo stesso, come peraltro evidenziato da PagoPA nella determinazione di acquisto, rappresenta uno "*strumento di analisi dei prodotti tecnologici volto a comprendere il comportamento degli utenti dei singoli prodotti, a visualizzarne, segmentarne ed analizzarne i dati, al fine di misurarne il successo e la diffusione e individuarne, per questa strada, aree di miglioramento*" ed "*è in grado di offrire informazioni dettagliate e in tempo reale su come le persone interagiscono con l'App in modo da potersi concentrare sulle funzionalità di maggior impatto e innovare più velocemente i servizi digitali resi disponibili al cittadino sull'App*" (cfr. all. D.01 alla relazione di servizio del 27 maggio 2021).

Le librerie di tracciamento di Mixpanel presenti all'interno dell'App IO sono, infatti, configurate per inviare automaticamente e sistematicamente i dati relativi a una pluralità di eventi (generati nel corso dell'utilizzo dell'app da parte dell'utente) ai sistemi di Mixpanel unitamente a un identificativo unico dell'utente. Le librerie di Mixpanel comportano, pertanto, un monitoraggio sistematico dell'utilizzo dell'App IO da parte degli utenti, trattamento che non risulta necessario per il perseguimento delle asserite finalità di "*assistenza, debug e miglioramento dell'App IO*" né strettamente necessario per erogare servizi esplicitamente richiesti da un utente nell'ambito dell'App IO. Ciò, senza che l'utente sia adeguatamente informato di tale circostanza o che possa esprimere il proprio consenso previsto dall'art. 122 del Codice.

Con riferimento, infine, all'utilizzo di Instabug, si evidenzia che lo stesso, come peraltro evidenziato da PagoPA nella determinazione di acquisto, rappresenta un "*software che fornisce feedback in-app e creazione di report sui bug alle applicazioni per dispositivi mobili e che implementa potenti tattiche per risolvere rapidamente i bug*" e che "*consente di avere una comunicazione bidirezionale senza interruzioni con utenti o tester, fornendo al contempo report dettagliati sull'ambiente per gli sviluppatori*" (cfr. all. C.02 alla relazione di servizio del 27 maggio 2021). In particolare, le librerie di Instabug richiamate nel codice sorgente dell'App IO sono configurate per archiviare nel terminale dell'utente diverse tipologie di informazioni (*User Attributes*, *Repros Steps*, *Session Profiler*, *Logs*, ivi inclusi gli eventi) e per accedere a tali informazioni nel caso in cui l'utente, all'interno dell'area "IO ti aiuto", effettui una segnalazione di eventuali problemi dell'app o invii suggerimenti per nuove funzionalità (allo stato non è stato possibile verificare se tali informazioni vengono accedute e inviate automaticamente a Instabug anche al verificarsi di un evento di *crash* dell'App IO). Ciò, senza che l'utente sia adeguatamente informato di tale circostanza o che possa esprimere il proprio consenso previsto dall'art. 122 del Codice.

Per tali ragioni, si ritiene che l'archiviazione all'interno del dispositivo dell'utente delle predette informazioni – non strettamente necessarie all'erogazione dei servizi dell'App IO – e il successivo accesso alle stesse avvengano quantomeno in violazione degli artt. 5, par. 1, lett. a), del Regolamento e 122 del Codice.

5.2. Sulla minimizzazione dei dati

Nel corso delle attività di analisi dinamica dell'App IO, è stato verificato che l'App IO è configurata per inviare ai sistemi di Mixpanel informazioni molto dettagliate in relazione ad alcune specifiche tipologie di servizi. Tali informazioni riguardano, tra le altre, il bonus vacanze dell'Agenzia delle entrate (es. eventi relativi alla verifica dei requisiti per la richiesta del bonus e alla generazione dello stesso), il programma *cashback* del Ministero dell'economa e finanze (es. elenco delle transazioni che partecipano al programma *cashback* e degli strumenti di pagamento elettronico dell'utente), nonché la piattaforma PagoPA (es. eventi relativi all'aggiunta di strumenti

di pagamento al portafoglio dell'utente e all'esecuzione di pagamenti a favore di pubbliche amministrazioni e gestori di pubblici servizi).

Con riferimento all'utilizzo delle librerie di Mixpanel, è inoltre emerso che l'identificativo utilizzato dalle stesse è generato mediante una funzione deterministica, peraltro resa pubblica (cfr. *repository* GitHub dell'App IO), che a partire dal codice fiscale di un utente produce sempre lo stesso risultato anche in caso di utilizzo di un diverso dispositivo mobile. Un siffatto identificativo univoco, in base alle sue caratteristiche, è qualificabile come un dato personale e può essere utilizzato per creare profili degli utenti dell'App IO e identificarli. Ricorrere alle predette modalità di attribuzione di un identificativo a ciascun utente dell'App IO non costituisce pertanto un'efficace misura di protezione dei dati, laddove si voglia impedire la reidentificazione dell'interessato. Ciò, in quanto tale identificativo presenta un elevato grado di associabilità al codice fiscale dell'utente, tenuto anche conto che, nel caso in esame, l'identificativo è trasmesso dall'App IO ai sistemi di Mixpanel unitamente all'indirizzo IP del dispositivo dell'utente e ad altre informazioni relative al suo dispositivo e agli eventi oggetto di tracciamento.

Al riguardo, PagoPA, nell'informativa resa agli utenti dell'App IO, rappresenta che sono utilizzati "*strumenti di tracciamento automatico che* […] *consentono di raccogliere dati relativi alle azioni che compi all'interno dell'App e dati relativi al tuo dispositivo (es. sistema operativo, modello del telefono, versione dell'App, indirizzo IP, area geografica). Questi dati sono raccolti tramite sistemi di fornitori terzi nominati responsabili del trattamento, e utilizzati esclusivamente per finalità di assistenza tecnica (dietro tua richiesta) e al fine elaborare statistiche sul funzionamento dei* […] *sistemi, e mediante l'adozione di meccanismi di pseudonimizzazione*". Tuttavia, per le ragioni sopra evidenziate, tali informazioni non risultano corrette in quanto i dati raccolti tramite gli strumenti di tracciamento presenti all'interno dell'App IO non possono essere considerati come dati sottoposti a pseudonimizzazione.

Tutto ciò premesso, si ritiene che la raccolta e i successivi trattamenti delle predette informazioni sui sistemi di Mixpanel non siano conformi al principio di minimizzazione dei dati in quanto i dati oggetto del trattamento non risultano essere adeguati, pertinenti e limitati a quanto necessario rispetto alle asserite finalità di *debug* e di assistenza tecnica all'utente dell'App IO, ponendosi in contrasto con il principio di "*minimizzazione dei dati*" di cui all'art. 5, par. 1, lett. c), del Regolamento.

5.3. Sul trasferimento di dati verso Paesi terzi

Ai fini della valutazione dei profili relativi al trasferimento di dati verso Paesi terzi, si rappresenta che dalla documentazione agli atti e dalle verifiche svolte è emerso che:

- Google si avvale di propri sistemi informatici (risorse elaborative e di *storage*), ubicati negli Stati Uniti e nell'Unione europea;
- Mixpanel si avvale di sistemi informatici (risorse elaborative e di *storage*) forniti da Google, ubicati negli Stati Uniti e nell'Unione europea;
- Instabug si avvale di sistemi informatici (risorse elaborative e di *storage*) forniti da Amazon Web Services, ubicati negli Stati Uniti.

Inoltre, risulta che le predette società si avvalgono, a loro volta, di altri fornitori di servizi (cfr. all. D.05, F, G e H alla relazione di servizio del 27 maggio 2021), alcuni dei quali sono anch'essi stabiliti in Paesi terzi.

Al riguardo, si evidenzia che, indipendentemente dal luogo in cui sono ubicati i sistemi informatici su cui conservati i dati personali degli utenti dell'App IO, l'accesso remoto a tali sistemi di trattamento da parte di soggetti stabiliti al di fuori dell'Unione europea (Google, Mixpanel e Instabug) configura comunque un trasferimento di dati verso Paesi terzi (cfr., sul punto, le "*Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al*

fine di garantire il rispetto del livello di protezione dei dati", adottate dal Comitato europeo per la protezione dei dati il 10 novembre 2020, spec. note 22 e 27).

5.4. Sulla protezione dei dati fin dalla progettazione e per impostazione predefinita

Nel corso delle attività di analisi dinamica dell'App IO, è stato verificato che la stessa è stata progettata e realizzata senza integrare nel trattamento le garanzie necessarie a soddisfare i requisiti del Regolamento e adottare misure tecniche e organizzative volte ad attuare in modo efficace i principi di protezione dei dati (principio della "*protezione dei dati fin dalla progettazione*", art. 25, par. 1, del Regolamento), nonché senza mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati necessari per ogni specifica finalità del trattamento (principio della "*protezione dei dati per impostazione predefinita*", art. 25, par. 2, del Regolamento). In particolare, è emerso che l'App IO è stata configurata senza tenere conto di elementi chiave dalla progettazione e dell'impostazione predefinita relativi a:

a) il principio della "*liceità, correttezza e trasparenza*", con riguardo all'adozione di misure volte a richiedere il consenso dell'utente dell'App IO all'archiviazione di informazioni sul proprio terminale e all'accesso ai dati ivi archiviati (cfr. par. 5.1), nonché alla configurazione dell'App IO evitando il conferimento a fornitori esterni di dati riferibili ai suoi utenti (cfr. par. 3.2);
b) il principio della "*minimizzazione dei dati*", con riguardo all'adozione di misure volte a garantire che i dati personali trattati sono pertinenti e necessari per le finalità perseguite, nonché a pseudonimizzare i dati personali quando non è necessario disporre di dati personali riferiti a persone fisiche identificate o identificabili (cfr. par. 5.2).

In primo luogo, si osserva infatti che, in base al principio della "*protezione dei dati fin dalla progettazione*" (art. 25, par. 1, del Regolamento), il titolare del trattamento deve adottare misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati (tra i quali i principi di "*liceità, correttezza e trasparenza*" e di "*minimizzazione dei dati*") e deve integrare nel trattamento le necessarie garanzie per soddisfare i requisiti del Regolamento e tutelare i diritti e le libertà degli interessati. Tale obbligo si estende anche ai trattamenti svolti per mezzo di un responsabile del trattamento. Infatti, le operazioni di trattamento effettuate da un responsabile dovrebbero essere regolarmente esaminate e valutate dal titolare per garantire che continuino a rispettare i principi e permettano al titolare di adempiere gli obblighi previsti dal Regolamento (cfr. "*Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita*", adottate il 20 ottobre 2020 dal Comitato europeo per la protezione dei dati, spec. punti 7 e 39).

In secondo luogo, occorre tener presente che, in conformità al principio della "*protezione dei dati per impostazione predefinita*" (art. 25, par. 2, del Regolamento), il titolare deve effettuare, assumendosene la responsabilità, scelte tali da garantire che venga effettuato per impostazione predefinita solo il trattamento strettamente necessario per conseguire una specifica e lecita finalità. Ciò significa che, per impostazione predefinita, il titolare del trattamento non deve raccogliere dati personali che non sono necessari per la specifica finalità del trattamento.

In tale ottica, il titolare è tenuto a definire in anticipo per quali finalità i dati personali vengono raccolti e trattati. Le misure devono, per impostazione predefinita, essere adeguate a garantire che siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento. Anche quando utilizza prodotti o servizi realizzati da terzi, il titolare del trattamento deve eseguire una valutazione dei rischi e accertarsi che siano disattivate le funzioni che non hanno una base giuridica o non sono compatibili con le finalità del trattamento.

In particolare, il titolare del trattamento deve tenere conto sia del volume dei dati personali sia delle tipologie, delle categorie e del livello di dettaglio dei dati personali necessari per le finalità

del trattamento. Le scelte effettuate dal titolare nella progettazione di un trattamento devono tenere conto dei maggiori rischi per i principi di integrità e riservatezza, di minimizzazione dei dati e della limitazione della conservazione connessi alla raccolta di grandi quantità di dati personali dettagliati, rispetto ai minori rischi associati alla raccolta di quantità minori di dati o di informazioni meno dettagliate sugli interessati. In ogni caso, le impostazioni predefinite non devono includere la raccolta di dati personali che non sono necessari per le finalità del trattamento. Non devono essere raccolte categorie di dati personali che sono superflue o dati di dettaglio che non sono necessari (cfr. "*Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita*", adottate il 20 ottobre 2020 dal Comitato europeo per la protezione dei dati, spec. punti 42, 43, 44 e 49).

ALLEGATO 1

Elenco degli eventi oggetto di tracciamento mediante librerie di Mixpanel

Evento oggetto di tracciamento	Tipologia "event"
Cambio dello stato dell'app	APP_STATE_CHANGE
Cambio della sezione dell'app	SCREEN_CHANGE
Login/logout dell'utente	ANALYTICS_AUTENTICATION_STARTED ANALYTICS_AUTENTICATION_COMPLETED LOGIN_SUCCESS LOGIN_FAILURE LOGOUT_REQUEST LOGOUT_SUCCESS SESSION_INFO_LOAD_SUCCESS SESSION_INFO_LOAD_FAILURE
Autenticazione SPID	IDP_SELECTED AUTHENTICATION_WEBVIEW_URL_CHANGED
Autenticazione CIE	CIE_AUTHENTICATION_ERROR CIE_HAS_API_LEVEL_REQUEST CIE_HAS_API_LEVEL_SUCCESS CIE_HAS_API_LEVEL_FAILURE CIE_HAS_NFC_FEATURE_REQUEST CIE_HAS_NFC_FEATURE_SUCCESS CIE_HAS_NFC_FEATURE_FAILURE CIE_IS_SUPPORTED_REQUEST CIE_IS_SUPPORTED_SUCCESS CIE_IS_SUPPORTED_FAILURE NFC_IS_ENABLED_REQUEST NFC_IS_ENABLED_SUCCESS NFC_IS_ENABLED_FAILURE UPDATE_READING_STATE_REQUEST UPDATE_READING_STATE_SUCCESS UPDATE_READING_STATE_FAILURE
Eventi connessi al bonus vacanza	BONUS_VACANZE_LOAD_ALL_ACTIVATION_REQUEST BONUS_VACANZE_LOAD_ALL_ACTIVATION_SUCCESS BONUS_VACANZE_LOAD_ALL_ACTIVATION_FAILURE BONUSES_AVAILABLE_REQUEST BONUSES_AVAILABLE_SUCCESS BONUSES_AVAILABLE_FAILURE BONUS_VACANZE_CHECK_ELIGIBILITY_REQUEST BONUS_VACANZE_CHECK_ELIGIBILITY_SUCCESS BONUS_VACANZE_CHECK_ELIGIBILITY_FAILURE BONUS_VACANZE_ACTIVATION_REQUEST BONUS_VACANZE_ACTIVATION_SUCCESS BONUS_VACANZE_ACTIVATION_FAILURE BONUS_VACANZE_REQUEST_CANCEL BONUS_VACANZE_ACTIVATION_COMPLETE BONUS_VACANZE_LOAD_FROM_ID_REQUEST BONUS_VACANZE_LOAD_FROM_ID_SUCCESS BONUS_VACANZE_LOAD_FROM_ID_FAILURE BONUS_VACANZE_FROM_ID_POLLING_START BONUS_VACANZE_FROM_ID_POLLING_CANCEL

Evento oggetto di tracciamento	Tipologia "event"
Eventi connessi al cashback	BPD_ENROLL_REQUEST BPD_ENROLL_SUCCESS BPD_ENROLL_FAILURE BPD_DELETE_REQUEST BPD_DELETE_SUCCESS BPD_DELETE_FAILURE BPD_UNSUBSCRIBE_COMPLETED BPD_UNSUBSCRIBE_COMPLETED_WITH_FAILURE BPD_ONBOARDING_START BPD_ONBOARDING_CANCEL BPD_ONBOARDING_COMPLETED BPD_ONBOARDING_USER_ACTIVATE BPD_ONBOARDING_ACCEPT_DECLARATION BPD_UPSERT_IBAN_REQUEST BPD_UPSERT_IBAN_SUCCESS BPD_UPSERT_IBAN_FAILURE BPD_IBAN_INSERTION_START BPD_IBAN_INSERTION_CONTINUE BPD_IBAN_INSERTION_CANCEL BPD_IBAN_INSERTION_RESET_SCREEN BPD_LOAD_ACTIVATION_STATUS_REQUEST BPD_LOAD_ACTIVATION_STATUS_SUCCESS BPD_LOAD_ACTIVATION_STATUS_FAILURE BPD_SELECT_PERIOD BPD_PERIODS_REQUEST BPD_PERIODS_SUCCESS BPD_PERIODS_FAILURE BPD_RANKING_REQUEST BPD_RANKING_SUCCESS BPD_RANKING_FAILURE BPD_AMOUNT_REQUEST BPD_AMOUNT_SUCCESS BPD_AMOUNT_FAILURE BPD_ALL_DATA_REQUEST BPD_ALL_DATA_SUCCESS BPD_ALL_DATA_FAILURE BPD_TRANSACTIONS_REQUEST BPD_TRANSACTIONS_SUCCESS BPD_TRANSACTIONS_FAILURE BPD_TRANSACTIONS_PAGE_REQUEST BPD_TRANSACTIONS_PAGE_SUCCESS BPD_TRANSACTIONS_PAGE_FAILURE BPD_PAYMENT_METHOD_ACTIVATION_REQUEST BPD_PAYMENT_METHOD_ACTIVATION_SUCCESS BPD_PAYMENT_METHOD_ACTIVATION_FAILURE

Evento oggetto di tracciamento	Tipologia "event"
Eventi connessi alla piattaforma PagoPA	WALLETS_LOAD_REQUEST WALLETS_LOAD_SUCCESS WALLETS_LOAD_FAILURE WALLET_LOAD_ABI_REQUEST WALLET_LOAD_ABI_SUCCESS WALLET_LOAD_ABI_FAILURE WALLET_ONBOARDING_BANCOMAT_LOAD_PANS_REQUEST WALLET_ONBOARDING_BANCOMAT_LOAD_PANS_SUCCESS WALLET_ONBOARDING_BANCOMAT_LOAD_PANS_FAILURE WALLET_ONBOARDING_BANCOMAT_ADD_REQUEST WALLET_ONBOARDING_BANCOMAT_ADD_SUCCESS WALLET_ONBOARDING_BANCOMAT_ADD_FAILURE WALLET_ONBOARDING_BANCOMAT_START WALLET_ONBOARDING_BANCOMAT_COMPLETED WALLET_ONBOARDING_BANCOMAT_COMPLETE PAYMENT_INITIALIZE_STATE PAYMENT_ENTRYPOINT_ROUTE BACK_TO_PAYMENT_ENTRYPOINT_ROUTE PAYMENT_VERIFICA_REQUEST PAYMENT_VERIFICA_SUCCESS PAYMENT_VERIFICA_FAILURE PAYMENT_ATTIVA_REQUEST PAYMENT_ATTIVA_SUCCESS PAYMENT_ATTIVA_FAILURE PAYMENT_ID_POLLING_REQUEST PAYMENT_ID_POLLING_SUCCESS PAYMENT_ID_POLLING_FAILURE PAYMENT_ID_TIMEOUT PAYMENT_CHECK_REQUEST PAYMENT_CHECK_SUCCESS PAYMENT_CHECK_FAILURE PAYMENT_FETCH_PSPS_FOR_PAYMENT_ID_REQUEST PAYMENT_FETCH_PSPS_FOR_PAYMENT_ID_SUCCESS PAYMENT_FETCH_PSPS_FOR_PAYMENT_ID_FAILURE PAYMENT_FETCH_ALL_PSPS_FOR_PAYMENT_ID_REQUEST PAYMENT_FETCH_ALL_PSPS_FOR_PAYMENT_ID_SUCCESS PAYMENT_FETCH_ALL_PSPS_FOR_PAYMENT_ID_FAILURE PAYMENT_UPDATE_WALLET_PSP_REQUEST PAYMENT_UPDATE_WALLET_PSP_SUCCESS PAYMENT_UPDATE_WALLET_PSP_FAILURE PAYMENT_EXECUTE_START_REQUEST PAYMENT_EXECUTE_START_SUCCESS PAYMENT_EXECUTE_START_FAILURE PAYMENT_WEB_VIEW_END PAYMENT_NAVIGATION_URLS PAYMENT_COMPLETED_SUCCESS PAYMENT_COMPLETED_FAILURE PAYMENT_DELETE_PAYMENT_REQUEST PAYMENT_DELETE_PAYMENT_SUCCESS PAYMENT_DELETE_PAYMENT_FAILURE PAYMENT_RUN_DELETE_ACTIVE_PAYMENT_SAGA PAYMENT_ABORT_RUNNING_PAYMENT PAYMENT_RUN_START_OR_RESUME_PAYMENT_ACTIVATION_SAGA