Guida Operativa

Sezione: Utilità

Campo	Valore
Piattaforma	GDPRLab
Sezione	Utilità
Destinatari	Consulenti tecnici / DPO / Rivenditori
Versione guida	1.0

1. Cos’è la sezione Utilità

La sezione Utilità mette a disposizione modelli di comunicazione precompilati da personalizzare e scaricare in PDF.

Si tratta di lettere di comunicazione destinate a specifici destinatari in caso di data breach o incidente informatico.

A differenza degli altri documenti della piattaforma (nomine, registri, autorizzazioni), i documenti generati da Utilità non vengono salvati nel repository con hash SHA-256: vengono generati, personalizzati e scaricati direttamente in PDF per un utilizzo immediato.

Si accede cliccando su **Utilità** nel menu laterale sinistro.

2. Struttura della pagina

La pagina mostra tre card, una per ogni template di comunicazione disponibile.

Ogni card riporta il titolo del template, una breve descrizione e il link **Genera e scarica PDF** per aprire il relativo editor.

3. I tre template disponibili

Template	Destinatari	Base normativa	Oggetto email predefinito
Comunicazione agli utenti di avvenuto data breach	Interessati al trattamento (clienti, dipendenti, fornitori, ecc.) i cui dati sono stati coinvolti nel breach	Art. 34 GDPR – Comunicazione agli interessati	Comunicazione importante relativa alla sicurezza dei suoi dati personali
Comunicazione interna di incidente informatico	Dipendenti e personale interno dell'organizzazione	Art. 32 GDPR – Misure di sicurezza; buone pratiche di incident management interno	Comunicazione interna di incidente informatico
Comunicazione data breach a fornitori	Fornitori e responsabili esterni del trattamento (art. 28 GDPR)	Art. 33 GDPR – Obbligo di cooperazione nella gestione del breach	Notifica di incidente di sicurezza informatica – richiesta verifiche

4. Funzionamento comune a tutti i template

Cliccando su una card si apre la modale dell'editor con la stessa struttura per tutti e tre i template:

→ **Avviso in giallo:** "Personalizza il testo e usa Genera PDF per scaricare il documento. Non viene salvato nel repository."

→ **Campo Oggetto email:** testo precompilato modificabile, che rappresenta l'oggetto della comunicazione

→ **Editor del corpo della lettera:** testo precompilato con la struttura completa della comunicazione, modificabile con la barra degli strumenti (H1, H2, H3, allineamento, tabelle, codice)

→ **Variabili disponibili:** tag in fondo all'editor

→ **Pulsante Genera PDF:** genera e scarica il documento in PDF

→ **Pulsante Chiudi:** chiude la modale senza generare il PDF

> **Attenzione: I documenti generati da Utilità NON vengono salvati nel repository con hash SHA-256. Se si necessita di conservare una copia certificata della comunicazione inviata, scaricare il PDF e archiviarlo manualmente nel repository tramite la funzione di upload (se disponibile) o in un sistema di archiviazione esterno.**

5. Template 1 – Comunicazione agli utenti di avvenuto data breach

Destinatari e scopo

Questa comunicazione è indirizzata agli interessati al trattamento (clienti, utenti, dipendenti) i cui dati personali sono stati coinvolti in un data breach.

È il documento con cui il Titolare adempie all'obbligo di comunicazione agli interessati previsto dall'art. 34 GDPR, quando il breach può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Struttura della lettera precompilata

Sezione	Contenuto
Intestazione	Comunicazione da parte del Titolare del trattamento agli interessati
1. Cosa è accaduto	Descrizione dell'incidente: data, modalità di accesso non autorizzato, sistemi coinvolti, periodo dell'evento
2. Quali dati potrebbero essere coinvolti	Elenco dei dati potenzialmente compromessi (es. nome e cognome, indirizzo email, numero di telefono) e dati confermati come non coinvolti (es. password, dati bancari, documenti identità)
3. Possibili conseguenze	Rischi per gli interessati: contatti fraudolenti, phishing, smishing, tentativi di impersonificazione
4. Cosa abbiamo fatto	Azioni immediate intraprese dal Titolare: blocco account, reset credenziali, indagine tecnica, rafforzamento controlli, notifica al Garante, misure sui fornitori
5. Cosa Le consigliamo di fare	Raccomandazioni agli interessati: attenzione a email/SMS sospetti, non comunicare password, verificare l'identità del mittente, controllare comunicazioni anomale. Link a risorse: www.acn.gov.it, www.garanteprivacy.it
6. Assistenza e contatti	Dati del Titolare del trattamento e del DPO per richiedere informazioni
7. Il nostro impegno	Dichiarazione di responsabilità e impegno del Titolare

> ***Nota operativa:*** *Questa comunicazione va inviata senza ingiustificato ritardo agli interessati quando il breach può presentare un rischio elevato (art. 34 GDPR). Personalizzare con cura le sezioni 1 e 2 con i dati reali dell'incidente prima di generare e inviare il PDF.*

6

6. Template 2 – Comunicazione interna di incidente informatico

Destinatari e scopo

Questa comunicazione è destinata al personale interno dell'organizzazione (dipendenti, collaboratori) per informarli di un incidente informatico che li riguarda o che potrebbe averli coinvolti.

Ha una finalità informativa e preventiva: informa i dipendenti dell'accaduto e fornisce istruzioni operative per ridurre il rischio di ulteriori danni.

Struttura della lettera precompilata

Sezione	Contenuto
Intestazione	Comunicazione interna riservata
1. Descrizione dell'evento	Data e modalità dell'incidente, sistemi coinvolti, accertamenti tecnici effettuati
2. Dati potenzialmente coinvolti	Tipologie di informazioni che potrebbero essere state compromesse (es. comunicazioni operative, contatti professionali, documenti gestionali)
3. Misure adottate	Azioni immediate: disattivazione credenziali, cambio password forzato, attivazione controlli rafforzati, analisi forense, comunicazione al Garante, aggiornamento configurazioni
4. Azioni richieste al personale	Istruzioni per i dipendenti: cambio password immediato, non riutilizzo su altri servizi, non comunicare credenziali, attenzione a email sospette, segnalazione immediata di anomalie
5. Collaborazione e responsabilità	Richiesta di collaborazione e canali di segnalazione interni

> ***Nota operativa:*** *Questa comunicazione è ad uso interno e non ha obblighi normativi diretti (non è la comunicazione agli interessati ex art. 34 né la notifica al Garante ex art. 33). Rappresenta una buona pratica di incident management interno e contribuisce a ridurre i rischi secondari derivanti dall'incidente.*

7. Template 3 – Comunicazione data breach a fornitori

Destinatari e scopo

Questa comunicazione è indirizzata ai fornitori e ai responsabili esterni del trattamento (soggetti ex art. 28 GDPR) per informarli di un incidente di sicurezza che ha coinvolto sistemi condivisi o dati che transitano attraverso i loro servizi.

Ha lo scopo di richiedere la loro cooperazione nelle verifiche e nelle misure di contenimento.

Struttura della lettera precompilata

Sezione	Contenuto
Intestazione	Comunicazione formale al Fornitore/Responsabile esterno
1. Natura dell'incidente	Tipo di accesso non autorizzato, data dell'evento, contenimento immediato, esclusione di interruzioni operative
2. Misure adottate	Azioni del Titolare: isolamento sistemi, revoca credenziali, rafforzamento autenticazione, verifiche tecniche, notifica autorità
3. Azioni richieste al fornitore	Richiesta di cooperazione: verifica accessi anomali ai sistemi collegati, controllo log per il periodo indicato, modifica credenziali condivise, conferma esito verifiche, segnalazione di anomalie rilevate
4. Cooperazione	Richiesta formale di cooperazione ai sensi della normativa privacy; canali di riferimento per la comunicazione

> ***Nota operativa:*** *Inviare questa comunicazione ai fornitori che forniscono servizi connessi ai sistemi coinvolti nell'incidente. La cooperazione del fornitore è fondamentale per determinare l'entità del breach e per evitare che l'incidente si propaghi attraverso i sistemi del fornitore stesso.*

8

8. Come usare i template: procedura operativa

→ Aprire il template cliccando sulla relativa card nella pagina Utilità

→ Leggere attentamente il testo precompilato: i dati del cliente (ragione sociale, email, telefono) vengono precompilati automaticamente dalla sezione Azienda

→ Personalizzare le sezioni specifiche dell'incidente: data, dati coinvolti, misure adottate (queste informazioni devono essere inserite manualmente in base all'incidente reale)

→ Modificare il campo Oggetto email se necessario

→ Cliccare **Genera PDF** per scaricare il documento

→ Inviare il PDF ai destinatari tramite email o altri canali appropriati

→ Conservare una copia del PDF inviato per documentazione interna

> ***Nota operativa:*** *Le variabili dinamiche visibili in fondo all'editor (mostrate come tag) vengono sostituite automaticamente con i dati dell'organizzazione al momento della generazione del PDF. Non è necessario sostituirle manualmente: compilare solo le sezioni specifiche dell'incidente (date, dati coinvolti, misure).*

9

9. Workflow consigliato in caso di data breach

La sezione Utilità va usata in coordinamento con il Registro Data Breach. Il flusso operativo raccomandato è:

→ Aprire l'incidente nel Registro Data Breach (documentazione interna obbligatoria)

→ Valutare se il breach richiede notifica al Garante (art. 33 GDPR – entro 72 ore)

→ Valutare se il breach richiede comunicazione agli interessati (art. 34 GDPR)

→ Se sì: aprire il template "Comunicazione agli utenti di avvenuto data breach", personalizzarlo e generare il PDF

→ Inviare la comunicazione interna al personale tramite il template "Comunicazione interna di incidente informatico"

→ Inviare la comunicazione ai fornitori coinvolti tramite "Comunicazione data breach a fornitori"

→ Aggiornare il Registro Data Breach con le azioni intraprese e lo stato di notifica

10

10. Relazioni con altre sezioni

Sezione	Relazione con Utilità
Registro Data Breach	La sezione Utilità fornisce i template di comunicazione da utilizzare in parallelo con la registrazione dell'incidente nel Registro Data Breach
Azienda	I dati del Titolare (ragione sociale, email, telefono) vengono precompilati automaticamente nelle lettere
Responsabili Esterni	I fornitori a cui va inviata la comunicazione data breach corrispondono ai Responsabili Esterni censiti nella piattaforma
Repository	I PDF generati da Utilità NON vengono salvati automaticamente nel repository: richiedono archiviazione manuale