POL-506 PERSONAL DATA BREACH RESPONSE POLICY

PURPOSE

This Data Breach Response Policy is documented to detail our approach for handling any potential threat to personal data, as well as taking appropriate action when the source of the intrusion or incident at a third party is traced back to the organization.
Incidents include virus infections, hacker attempts and break-ins, including disclosure of confidential information to others, system service interruptions, breach of personal information and other events with serious information security implications.
A personal data breach is defined as any MONEK or MONEK-affiliated company employee
becoming or being made aware of the actual or possible compromise of personal data and/or a non-compliance to this policy. It is the duty of all MONEK or MONEK-affiliated company employees to promptly inform MONEK senior management of any personal data
breach.

POLICY

Step 1: Notification

Where there are any suspicions of a threat or compromise to personal data, the DPO will be
notified immediately and they will be responsible for assembling and coordinating the activity of the Incident response team, the members of which will be determined by the nature of the incident but will always include a customer services representative responsible
for acting on behalf of our merchants and partners and their end customers.

MONEK Limited
F2 & F3 City Wharf, Davidson Road,
Lichfield, England, WS14 9DZ
T: +44 (0) 345 269 6645
W: www.monek.com

Step 2: Assess Incident Priority

The incident response team will identify the priority of the event measured by Impact and
Urgency based on the scope of the incident in terms of the type of data and volume of individuals concerned.

Step 3: Log the Incident

We will ensure that all incidents are immediately logged in our helpdesk system with a clear
definition of next steps, including timescales and individuals assigned ownership of each task.

Step 4: Manage The Incident

We will ensure the correct use of available resources to address the issue with the highest
priority and call in additional resources as required.
We will ensure someone records the timeline, events and actions taken for post-incident analysis and that all decisions have been correctly assessed for risk and impact.

Step 5: Establish Timetable for Communication

Relative to the priority of the incident and the impact assessment, we will inform clients at the
level appropriate to the severity and nature of the incident using our Personal Data Breach
Notification Template (See Appendix 1)
We will ensure there is a clear schedule for client communication, and that updates are posted in strict accordance with the schedule and will always follow an announcement with
a statement such as ". We will provide an update at xx:xx".
Any breach of personal data will be reported to the ICO within 72 hours – see

Guide to the UK General Data Protection Regulation (UK GDPR)
gdpr/personal-data-breaches/

MONEK Limited
F2 & F3 City Wharf, Davidson Road,
Lichfield, England, WS14 9DZ
T: +44 (0) 345 269 6645
W: www.monek.com

Step 6: Resumption of Normal Operations

Once the issue has been thoroughly investigated and all actions completed, we will relay this
back to our clients with a full root cause report to include as necessary details of the issue,
resolution and any corrective actions which will be taken to improve the situation.

Step 7: Post-Incident Analysis

In the days following the Incident, we will conduct a post-incident analysis to review how the
Incident was handled and whether any lessons could be learned from the situation and identify whether any changes are required to our Incident Process to better manage a repeat of the Incident / mitigate any further occurrences.

INTRODUCTION

This document is designed to advise of and provide an explanation regarding a potential or confirmed breach of Personal Data relating
to the service detailed below. A definition of the breach will be stated and clear guidance on how the fault was resolved is provided.
This document does not seek to apportion responsibility or liability for any parties referred to within and is provided without prejudice.

MONEK Limited
F2 & F3 City Wharf, Davidson Road,
Lichfield, England, WS14 9DZ
T: +44 (0) 345 269 6645
W: www.monek.com

DETAIL	
Summary	
Incident Reference	
Incident Manager	
Service Affected	
Incident Date and Time	
Date Reported to ICO	
Reported to Monek by Customer	
Time of Resolution	
Total Incident Window	
Description of Incident	
Incident Details	
Immediate cause	
Scope of the exposure	
Categories and approx. no. of individuals	
Categories and approx. no. of records	
Outside Involvement, from whom?	
Cause & Fault Resolution	
Cause	
How was cause identified?	
What work took place to resolve the incident?	

MONEK Limited
F2 & F3 City Wharf, Davidson Road,
Lichfield, England, WS14 9DZ
T: +44 (0) 345 269 6645
W: www.monek.com

How have lessons learnt been incorporated?	
Further commentary on risk	
ICO notification reference	

MONEK Limited
F2 & F3 City Wharf, Davidson Road,
Lichfield, England, WS14 9DZ
T: +44 (0) 345 269 6645
W: www.monek.com