Bayerisches Landesamt für
Datenschutzaufsicht

Bayer. Landesamt für Datenschutzaufsicht | Postfach 606 | 91511 Ansbach

Herr Dieter Adolf Kölbel
[redacted]

Bayerisches Landesamt für
Datenschutzaufsicht
Promenade 18 | 91522 Ansbach
Telefon: 0981 180093 0
Fax: 0981 180093 800
E-Mail: poststelle@lda.bayern.de
Web: www.lda.bayern.de

Ihre Kontaktperson
[redacted]
Telefon: 0981 180093 [redacted]
Fax: 0981 180093 842

| Ihr Zeichen / Ihr Schreiben vom | Unser Aktenzeichen |
|---|---|
| / | LDA-1085.4-3632/22-T |

Ansbach, 31.05.2022

## Datenschutzbeschwerde nach Art. 77 Datenschutz-Grundverordnung (DS-GVO)

### Abschlussmitteilung

Sehr geehrter Herr Kölbel,

mit diesem Schreiben kommen wir auf Ihre Beschwerde vom 02.05.2022, die bei uns am 05.05.2022 eingegangen ist, zurück. Wir haben Ihren Beschwerdesachverhalt unter dem Aktenzeichen LDA-1085.4-3632/22-T geprüft und stellen fest, dass der von Ihnen geschilderte Beschwerdesachverhalt im Kern deckungsgleich mit einer Vielzahl bereits vorliegender Meldungen ist. Durch das gehäufte Auftreten vergleichbarer Meldungen in der Vergangenheit, haben wir den Verantwortlichen PAYBACK GmbH (nachfolgend „PAYBACK"), gegen den sich Ihre Beschwerde richtet, bereits im Rahmen eines Verfahrens nach Art. 58 DS-GVO datenschutzrechtlich überprüft.

Im Rahmen dieser datenschutzrechtlichen Untersuchungen wurden zunächst allgemeine Sicherheitsaspekte bezüglich des Einlösens von Treuepunkten bei PAYBACK hinsichtlich den Vorgaben aus Art. 32 DS-GVO zur Sicherheit der Verarbeitung abgefragt. PAYBACK konnte uns darlegen, dass eine Einlösung von Treuepunkten lediglich nach erfolgreicher Authentifizierung möglich sei. Eine Einlösung ohne Authentifizierung ist nach derzeitigen Erkenntnissen zu keiner Zeit möglich. Bei unserer Überprüfung im Bereich einer möglichen Legitimation über die verfügbaren Authentifizierungsverfahren konnten wir keine Hinweise auf technische oder organisatorische Mängel entgegen den Vorschriften aus Art. 32 DS-GVO feststellen.

Neben der Prüfung des allgemeinen Prozesses zum Einlösen von Treuepunkten haben wir PAYBACK des Weiteren dazu aufgefordert, die uns vorliegenden Beschwerdesachverhalte im Detail zu untersuchen und den Weg der unberechtigten Einlösung durch einen Dritten prozessual nachzuzeichnen. Die Schwerpunkte unserer Untersuchung betrafen das ausgewählte Einlöseverfahren und den Umstand, ob für das entsprechende Kundenkonto ein persönliches Passwort gewählt wurde. Das Wählen eines persönlichen Passwortes hat eine herausragende Bedeutung als Schutzfunktion insofern, dass nach Setzen eines Passwortes die Möglichkeit zur Einlösung von Treuepunkten alleine mittels Geburtsdatum und Postleitzahl in den meisten Fällen nicht mehr möglich ist. Es wurde festgestellt, dass in den untersuchten Einzelfällen jeweils ein persönliches Passwort für das zugehörige Kundenkonto erstellt wurde. Das bedeutet, dass eine Einlösung von Treuepunkten lediglich mit dem gewählten Passwort oder der gewählten PIN möglich war. Bei einer Offline-Einlösung von Treuepunkten über die Kanäle

Hinweise zur Verarbeitung Ihrer personenbezogenen Daten:
Verantwortlich für die Verarbeitung Ihrer personenbezogenen Daten im Rahmen des vorliegenden Kontakts ist das Bayerische Landesamt für Datenschutzaufsicht. Weitere Informationen zur Verarbeitung Ihrer Daten, insbesondere zu den Ihnen zustehenden Rechten, können Sie unserer Homepage unter www.lda.bayern.de/Informationen entnehmen oder auf jedem anderen Wege unter den o.g. Kontaktdaten bei uns erfragen.

Dieter Adolf Kölbel
[redacted]

Bayerisches Landesamtes für Datenschutzaufsicht
Postfach 1349

91504 Ansbach

2. Mai 2022

**Vermutliches Datenleck bei dem Unternehmen**
**Payback GmbH, Theresienhöhe 12, 80339 München**

Sehr geehrte Damen und Herren,

am 21. März 2022 erhielt ich vom vorgenannten Unternehmen eine Nachricht, dass eine Prämienbestellung von meinem Account ausgeführt wurde. Da dies nicht durch mich erfolgte, habe ich taggleich um 15:10 h mein Passwort geändert, dass Unternehmen informiert und angefragt die getätigten Bestellungen rückgängig zu machen. Dies lehnte Payback ab. Auf meine nachfolgende Anfrage, wie Dritte an meine Zugangsdaten gelangt sein können, wird nicht wirklich eingegangen, bzw. wird lapidar bestritten, dass es bei der Payback GmbH ein Datenleck gibt oder gab. Zeitgleich mit der o. g. Aktivität begann eine massive Spam-Attacke auf mein Postfach d.koelbel@koelbels.de, welche eben jene Vermutung nahelegt, dass das Datenleck nicht bei mir, sondern beim genannten Unternehmen zu suchen ist.

Die Payback GmbH weist alle Vorwürfe zurück und verschickt einfach Standardschreiben mit Standardtextbausteinen an mich. Man ist schlicht nicht bereit, sich mit der Möglichkeit selbst Opfer zu sein, auseinanderzusetzten, obwohl die Sicherheitsstandards des Unternehmens als mehr als lausig zu betrachten sind, denn wo sonst ist denn heute noch ein Login mit Postleitzahl und Geburtsdatum möglich?

Ich bitte Sie höflichst die Sicherheitsstandards der Payback GmbH im Hinblick auf die Datenschutzrechte von Verbrauchern zu überprüfen. Meinen Schriftverkehr füge ich diesem Schreiben in Kopie an.

Mit freundlichen Grüßen,

Dieter-Adolf Kölbel

PAYBACK

PAYBACK.de

PAYBACK Service Center, Postfach 23 21 02, 85330 München

07 2FF1 6660 8F 1000 37BD
DV 04.22 0,85 Deutsche Post

*K4007*50622*0000891*04*

Dieter Kölbel
[redacted]
65719 Hofheim am Taunus

4. April 2022

L00850622 S00000891 B123456
D001-SB1 P0001-0001 B

**Ihre Kundennumme: 3083422193830437**
**Die Einlösung Ihrer PAYBACK Punkte**

Hallo Dieter Kölbel,

Sie haben uns vor kurzem über eine Einlösung von PAYBACK Punkten informiert, die Sie nicht selbst veranlasst hatten. Wir haben Ihr Anliegen im Detail geprüft und möchten Sie gerne über Folgendes informieren:

Die Einlösung von PAYBACK Punkten funktioniert durch das Eingeben Ihrer Postleitzahl in Kombination mit Ihrem Geburtsdatum bzw. Ihrer selbst gewählten PAYBACK PIN oder durch die Eingabe Ihrer Kundennummer/E-Mail Adresse und dem Passwort. Die PAYBACK Karte kann dabei auch digital (z.B. mithilfe von Apps) vorgezeigt werden. Die Person, die die Einlösung durchgeführt hat, war demnach im Besitz Ihrer Login-Daten.

Wir prüfen unsere Systeme kontinuierlich und haben keinen unerlaubten Zugriff auf unsere Systeme festgestellt - es liegt also kein Sicherheitsproblem bei PAYBACK vor. Wir gehen daher davon aus, dass entweder unbekannte Dritte über gefälschte E-Mails (Phishing-E-Mails) an Ihre persönlichen Daten gelangt sind oder dass jemand Ihre E-Mail- und Passwort-Kombination woanders ausgespäht hat. Wenn Sie dieselben Login-Daten für mehrere Online-Dienste – und auch PAYBACK - nutzen, ist auf diesem Weg auch ein Login in Ihr PAYBACK Konto möglich.

Wir empfehlen Ihnen dringend, das Passwort für Ihr E-Mail Konto zu ändern. Achten Sie dabei insbesondere auf die Auswahl eines sicheren Passworts (z.B. Verwendung von Groß-/Kleinschreibung, Sonderzeichen, Ziffern etc).

Zur Rückerstattung Ihrer PAYBACK Punkte können wir Ihnen Folgendes mitteilen:

Laut unseren Teilnahmebedingungen haften wir für entstandene Schäden nur bei grobem Verschulden unsererseits - dies liegt nicht vor. Da uns Ihre Zufriedenheit als Kunde jedoch sehr wichtig ist, haben wir uns ohne Anerkennung einer Rechtspflicht entschieden, die Punkte einmalig aus Kulanz gutzuschreiben. Die Gutschrift erfolgt innerhalb der nächsten 7 Werktage.

Mit freundlichen Grüßen
[redacted]
Vom PAYBACK Kundenservice



Dieter Adolf Kölbel
[redacted]

PAYBACK GmbH
Theresienhöhe 12

80339 München

31. März 2022

**Ihre Schreiben vom 23. März 2022 und 28. März 2022**
**Kundennummer 3083422193830437**

Sehr geehrte Damen und Herren,

ich gehe im Gegensatz zu Ihnen nicht davon aus, dass mein Payback-Konto im klassischen Sinne durch meine Email und Passwort ausgespäht wurde. Vielmehr gehe ich davon aus, dass Sie gehackt wurden und entgegen Ihrer Verpflichtung Kunden proaktiv darüber zu informieren, dass der Schaden auf Ihrer Seite verursacht wurde, versuchen dem Kunden zu suggerieren die Verantwortung läge bei ihm. Ich weise Sie darauf hin, dass dies im Falle einer Anzeige erhebliche Konsequenzen für Ihr Unternehmen haben wird, da die Datenschützer diese Vorfälle streng ahnden.
Zur Erläuterung, die Attacke auf das o. g. Konto erfolgte zeitgleich mit einer massiven Spam-Attacke auf mein Postfach d.koelbel@koelbels.de, welche immer noch nicht vollständig abgeebbt ist. Dies deutet unter Berücksichtigung der Tatsache, dass fünf weitere Postfächer unter @koelbels.de nicht betroffen sind, darauf hin, dass meine Emailadresse in Ihrem System erbeutet wurde und nicht wie Sie behaupten, ein Dritter in den Besitz meiner Daten ohne Ihr Zutun gelangt ist.

Bevor ich mich an die Bundesnetzagentur wende und den Sachverhalt dort zur Anzeige bringe, gebe ich Ihnen hier die Gelegenheit im Sinne von Anstand und Gesetzestreue Stellung zu nehmen.

PAYBACK

PAYBACK.de

07 2FF1 6660 72 C000 0176
DV 03.22 0,85 Deutsche Post

*K4007*49399*0000023*29*

Dieter Kölbel
[redacted]
65719 Hofheim am Taunus

28. März 2022

**Ihre Kundennummer 2193830437**
**Ihre Anfrage zu Ihrem PAYBACK Punktekonto**

Hallo Dieter Kölbel,

vielen Dank, dass Sie sich mit Ihrem Anliegen an uns gewandt haben.

In Ihrem PAYBACK Konto wurden eine oder mehrere PAYBACK Punkte Einlösungen ausgelöst.

Die Einlösung von PAYBACK Punkten ist nur nach Login im PAYBACK Konto möglich. Je nach Einlösekanal werden für den Login Kundennummer und PIN bzw. Passwort bzw. Geburtsdatum und PLZ abgefragt. Der Einlöser war also im Besitz dieser Daten.

Wir prüfen unsere Systeme kontinuierlich und können einen Fremdzugriff auf unsere Systeme ausschließen. Wir müssen daher davon ausgehen, dass ein unbekannter Dritter Ihre Daten an anderer Stelle ausgespäht hat. Wenn Sie zum Beispiel diese Kombination aus E-Mail-Adresse und Passwort öfter nutzen und diese Kombination woanders ausgespäht wurde, würde der Login auf www.PAYBACK.de mit den ausgespähten Daten funktionieren. Alternativ können Dritte auch über Phishing-Mails Ihre persönlichen Daten erfahren haben. Weitere Informationen zu Phishing-Mails finden Sie unter https://www.PAYBACK.de/sicherheit.

So sichern Sie Ihre Daten wieder:

1. Ändern Sie schnell Ihre Zugangsdaten (Passwörter) für Ihren E-Mail-Account und ggf. auch für andere Online-Dienste.
2. Überprüfen Sie Ihren Computer oder andere Geräte auf Schadsoftware.

Aus Sicherheitsgründen haben wir Ihr PAYBACK Konto gesperrt. Damit wir Ihr Punktekonto wieder freischalten können, setzen Sie sich bitte telefonisch mit uns in Verbindung. Sie erreichen uns von Montag bis Samstag, 8 bis 20 Uhr unter der Rufnummer 089 / 540 20 80 20.

Vielen Dank für Ihr Verständnis und Ihre Mühe.

Mit freundlichen Grüßen

[redacted]

Vom PAYBACK Kundenservice

L00849399 D001-SB1 S00000023 P0001-0001 B123456 B

PAYBACK Service Center
Postfach 23 21 02, 85330 München, PAYBACK.de/kontakt

PAYBACK GmbH
Geschäftsführer: Bernhard Brugger, Dominik Dommick, Conrad Pozsgai
Amtsgericht und Sitz: München, HRB 135 999

PAYBACK

PAYBACK.de

PAYBACK Service Center, Postfach 23 21 02, 85330 München

07 2FF1 6660 5B 3000 3B20
DV 03.22 0,85 Deutsche Post

*K4007*48339*0000946*23*

Dieter Kölbel
[redacted]
65719 Hofheim am Taunus

23. März 2022

L00848339 S00000946 B123456
D0011-SB1 P0001-0001 B

**Ihre Kundennummer 3083422193830437**
**Wichtige Informationen zu Ihrem PAYBACK Konto**

Hallo Dieter Kölbel,

wir prüfen automatisiert und regelmäßig auffällige Login-Aktivitäten von PAYBACK Konten. Im Rahmen dieser automatisierten Überprüfungen haben wir in Bezug auf Ihr PAYBACK Konto Grund zur Annahme, dass ein Dritter im Besitz Ihrer Login-Daten sein könnte. Da wir keine Hinweise darauf bzw. Anzeichen dafür haben, dass unzulässig auf PAYBACK Systeme eingewirkt wurde, müssen wir daher davon ausgehen, dass ein unbekannter Dritter Ihre Daten an anderer Stelle ausgespäht haben und versucht haben könnte, die Kombination von E-Mail und Passwort zum Login in Ihr PAYBACK Konto auf www.PAYBACK.de zu nutzen.

Bitte überprüfen Sie daher unbedingt Ihren Computer oder andere Geräte auf Schadsoftware, um einen Missbrauch zu verhindern. Wir empfehlen Ihnen zudem, umgehend Ihre Passwörter für die Online-Dienste, die Sie nutzen, zu ändern. Wir schicken Ihnen wichtige Informationen des Bundesamts für Sicherheit in der Informationstechnik (BSI), die hilfreich sind, um sich wirksam vor Internet-Betrug zu schützen:

FAQ zu Identitätsdiebstahl: https://www.sicherheitstest.bsi.de/faq

Empfehlungen für Passwort-Sicherheit: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

Wir haben Ihr PAYBACK Konto vorsorglich gesperrt, um einen unberechtigten Zugriff durch Dritte auf Ihr PAYBACK Konto zu verhindern. Bitte setzen Sie sich mit uns in Verbindung, wir geben Ihr PAYBACK Konto dann frei, so dass Sie Ihr Passwort zurücksetzen können. Sie erreichen uns am besten unter 089 540 20 80 20 (Mo-Sa 08:00 - 20:00). Wenn der Sprachcomputer Ihr Anliegen nicht lösen kann, leitet er Sie an einen Service Mitarbeiter weiter.

Mit freundlichen Grüßen
[redacted]
Vom PAYBACK Kundenservice



3363

Dieter Adolf Kölbel
[redacted]

PAYBACK GmbH
Theresienhöhe 12

80339 München

21. März 2022

**Mein Payback-Konto 2402193830439**

**Kundennummer 219 383 0437**

Sehr geehrte Damen und Herren,

folgende Prämienbestellungen wurden nicht von mir getätigt. Ich habe mein Passwort um 15:10 h zurückgesetzt. Bitte stornieren Sie die Bestellungen.

| | | | |
|---|---|---|---|
| PRÄMIENSHOP | **21.03.2022**<br>Punkte eingelöst | | - 999 °P |
| ARAL | **21.03.2022**<br>Punkte sammeln | Coupons entdecken | + 34 °P |
| | ⓘ **Alle PAYBACK Services immer dabei!**<br>Die PAYBACK App ist der ganz persönliche Shopping-Begleiter. **Mehr erfahren** | | |
| ARAL | **21.03.2022**<br>2FACH °P auf Kraftstoffe und Erdgas!* | Coupons entdecken | + 34 °P |
| PRÄMIENSHOP | **20.03.2022**<br>Punkte eingelöst | | - 14.996 °P |

Mit freundlichen Grüßen,

Dieter Adolf Kölbel