Meldung einer Verletzung des Schutzes personenbezogener Daten (Art. 33 DS-GVO)

Bitte beachten Sie die Hinweise auf unserer Homepage:

https://www.ldi.nrw.de/mainmenu_Aktuelles/Formulare-und-Meldungen/

1. Art der Meldung (Art. 33 Abs. 4)

☒ Neumeldung Aktenzeichen T5.4-41480/22 Datum 2022.11.03 17:17:18

☐ Ergänzende Meldung

☐ Es stehen derzeit nicht alle Informationen zur Verfügung, eine ergänzende Meldung erfolgt voraussichtlich bis zum:

2. Verantwortlicher (Art. 4 Nr. 7)

Name	acardo activation gmbh
Straße	Am Kai 12
PLZ	44263 Ort Dortmund
Telefon	0231-584497-0
E-Mail	info@acardo.com
Art der Stelle	nichtöffentlich
Bereich	Sonstige Dienstleistungen

3. Meldende Person

Beziehung zum Verantwortlichen	Geschäftsführer
Name	[redacted]
Straße	Am Kai 25
PLZ	44263 Ort Dortmund
Telefon	0231-584497-[redacted]
E-Mail	[redacted]@acardo.com

4. Anlaufstelle für weitere Informationen (Art. 33 Abs. 3 lit. b)

☒ Meldende Person

☐ Datenschutzbeauftragter

☐ Andere Person

5. Weitere an der Verletzung des Schutzes personenbezogener Daten Beteiligte

An der Verletzung des Schutzes personenbezogener Daten sind Dritte (z.B. Auftragsverarbeiter (Art. 4 Nr. 8), gemeinsam Verantwortlicher (Art. 26 Abs. 1)) beteiligt. ☒ ja ☐ nein

Rolle des Dritten im Rahmen der Verarbeitung	Cloud-Anbieter
Name	Amazon Web Services EMEA SARL
Straße	38 avenue John F. Kennedy
PLZ	1855 Ort Luxembourg
Telefon	+352 2 789 0057
E-Mail	aws-EU-privacy@amazon.com

6. Bekanntwerden der Verletzung des Schutzes personenbezogener Daten

Zeitpunkt/-raum der Verletzung des Schutzes personenbezogener Daten:

☐ am

☒ von 19.09.2022 14:07 bis 03.11.2022 14:26

Zeitpunkt des Bekanntwerdens der Verletzung des Schutzes personenbezogener Daten: 03.11.2022 14:14

Begründung der Verzögerung, falls Meldung nicht binnen 72 Stunden erfolgt (Art. 33 Abs. 1)

Wie wurde die Verletzung des Schutzes personenbezogener Daten bekannt?

E-Mail von [redacted] vom Chaos Computer Club

7. Beschreibung der Verletzung des Schutzes personenbezogener Daten

Art der Verletzung des Schutzes personenbezogener Daten (Art. 33 Abs. 3 lit. a, Art. 4 Nr. 12)

- ☐ Vernichtung
- ☐ Verlust
- ☐ Veränderung
- ☐ Unbefugte Offenlegung
- ☒ Unbefugter Zugang

Erläuterung:

Es war möglich, ohne Zugangsdaten auf die Datenbank zuzugreifen.

Wie kam es zu der Verletzung des Schutzes personenbezogener Daten?

- ☐ Weitergabe von personenbezogenen Daten an Unbefugte
- ☐ Fehlversand
- ☐ Veröffentlichung
- ☐ Offener E-Mailverteiler
- ☐ Diebstahl eines Mediums mit personenbezogenen Daten
- ☐ Verlust eines Mediums mit personenbezogenen Daten
- ☐ Zerstörung eines Mediums mit personenbezogenen Daten
- ☐ Hackerangriff (Virus/Trojaner/Phishing)
- Fehlkonfiguration

Erläuterung:

Es wurde ein Datenbank-Nutzer ohne Zugangsdaten angelegt.

Wer oder was hat die Verletzung des Schutzes personenbezogener Daten ausgelöst?

- [ ] Technischer Fehler
- [ ] Person mit Schädigungsabsicht
- [ ] Person ohne Schädigungsabsicht
- [x] unbekannt

8. Beschreibung der betroffenen Personen und Daten

Kategorien betroffener Personen (Art. 33 Abs. 3 lit. a)

- [ ] Kinder/Minderjährige
- [ ] Kunden oder Kundinnen
- [ ] Beschäftigte
- [x] Nutzer oder Nutzerinnen
- [ ] Patienten oder Patientinnen
- [ ] schutzbedürftige Personen

Kategorien betroffener Daten (Art. 33 Abs. 3 lit. a)

Besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1)

- [ ] Daten zur rassischen und ethnischen Herkunft
- [ ] politische Meinungen
- [ ] religiöse oder weltanschauliche Überzeugungen
- [ ] Gewerkschaftszugehörigkeit
- [ ] genetische Daten
- [ ] biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person
- [ ] Gesundheitsdaten
- [ ] Daten zum Sexualleben oder zur sexuellen Orientierung

Sonstige Kategorien

- [x] Finanzdaten
- [ ] Daten aus dem Versicherungsbereich
- [x] E-Mail-Adressen
- [ ] Passwörter
- [ ] Geheimhaltungs- oder Verschwiegenheitspflichten unterliegende Daten
- [x] Postadressen
- [ ] Standortdaten
- [ ] Fotos/Videos

Ungefähre Zahl betroffener Personen (Art. 33 Abs. 3 lit. a): 500000

Ungefähre Zahl betroffener Datensätze (Art. 33 Abs. 3 lit. a): 500000

Ergänzende Bemerkungen

9. Folgen der Verletzung des Schutzes personenbezogener Daten

Welche Folgen hat die Verletzung des Schutzes personenbezogener Daten wahrscheinlich für die betroffenen Personen (Art. 33 Abs. 3 lit. c) ?

- [x] Identitätsdiebstahl
- [x] Betrug
- [ ] finanzielle Verluste
- [ ] Gefährdung des Berufsgeheimnisses
- [ ] Verlust der Kontrolle ihrer personenbezogener Daten
- [ ] Einschränkung von Rechten
- [ ] Diskriminierung
- [ ] Aufhebung der Pseudonymisierung
- [ ] Rufschädigung
- [ ] erhebliche wirtschaftliche Nachteile
- [ ] erhebliche gesellschaftliche Nachteile
- [ ] Gefahr für Leib und Leben

Erläuterung:

Es war theoretisch möglich, Namen, E-Mail-Adressen, Adressen und/oder Bankdaten unserer Nutzer auszulesen.

Welches Risiko für die Rechte und Freiheiten betroffener Personen besteht nach aktuellem Kenntnisstand voraussichtlich (Art. 33 Abs. 3 lit. c)?

- [ ] voraussichtlich kein bzw. nur geringes Risiko
- [x] Risiko
- [ ] hohes Risiko

Begründung:

Der Zugang zur Datenbank war zwar offen, es sind uns jedoch keine Tatsachen bekannt, die die Annahme rechtfertigen, dass dieser Zugang auch tatsächlich mißbräuchlich genutzt wurde. Theoretisch besteht aber das Risiko, dass auf die Daten unbefugt zugegriffen wurde.

10. Maßnahmen zur Behebung oder Abmilderung der Verletzung des Schutzes personenbezogener Daten

Wurde die Verletzung des Schutzes personenbezogener Daten beseitigt? [x] ja [ ] nein

Begründung:

Nach Bekanntwerden des offenen Zugangs wurde dieser innerhalb von 15 Minuten geschlossen.

Welche Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten hat der Verantwortliche ergriffen bzw. schlägt er vor (Art. 33 Abs. 3 lit. d)?

Wir haben ein Monitoring eingerichtet, dass derartige Fehlkonfigurationen in Zukunft überwacht und meldet. Weiterhin haben wir alle unsere Datenbanken auf ähnliche Schwachstellen geprüft, allerdings ohne weitere Funde.

Welche Maßnahmen zur Abmilderung möglicher nachteiliger Auswirkungen hat der Verantwortliche ergriffen bzw. schlägt er vor (Art. 33 Abs. 3 lit. d)?

11. Benachrichtigung der betroffenen Personen (Art. 34)

☒ Die betroffenen Personen wurden nicht benachrichtigt, da voraussichtlich kein hohes Risiko für die Rechte und Freiheiten betroffener Personen besteht.

☐ Die betroffenen Personen wurden benachrichtigt (Art. 34 Abs. 1)

12. Betroffenheit weiterer Aufsichtsbehörden der Bundesländer

☐ Niederlassungen in weiteren Bundesländern sind von der Verletzung des Schutzes personenbezogener Daten betroffen.

13. Grenzüberschreitende Verarbeitung (Art. 4 Nr. 23)

☐ Es handelt sich um eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten von Niederlassungen eines Verantwortlichen oder eines Auftragsverarbeiter in mehr als einem Mitgliedstaat nach Art. 4 Nr. 23 lit. a erfolgt.

☐ Es handelt sich um eine Verarbeitung personenbezogener Daten die erhebliche Auswirkungen auf betroffene Personen aus dem Bereich weiterer EU-Staaten / Europäischer Wirtschaftsraum (EWR) Mitgliedsstaaten nach Art. 4 Abs. 23 lit. b hat oder haben kann.

14. Anlagen

Nr.	Dateiname	Datum	Größe
1	02 20221123 Information Betroffene.pdf	25.11.2022	1.09 MB
2	03 2022-11-03_SecurityIncident-231122-1736.pdf	25.11.2022	65.01 kB

Neumeldung

1. Angaben zur Meldung

Aktenzeichen	T5.4-41480/22
Eingangsdatum	03.11.2022 17:17:18
Verantwortlicher	acardo activation gmbh
Korrektur Art der Stelle	nicht-öffentlich
Korrektur Bereich	Sonstige Dienstleistungen

2. Anlaufstelle für weitere Informationen

Name	[redacted]
Anrede	Herr
Beziehung zum Verantwortlichen	Geschäftsführer
E-Mail Kontakt	[redacted]@acardo.com

3. Status der Bearbeitung

Status	abgeschlossen
Im Status seit	25.11.2022 15:12:43
Bearbeiter	[redacted]
Frist	25.11.2022
Bemerkungen	Da es keine weiteren Anhaltspunkte auf einen unberechtigten Zugriff gibt, die Betroffenen aber dennoch informiert wurden, kann der Vorgang abgeschlossen werden. Den Petenten aus der Beschwerde werde ich ebenfalls informieren. Viele Grüße [redacted]

#	Sachbearbeiter	Status	Datum Letzte Änderung	Frist	Bemerkungen
1	[redacted]	Antrag gestellt	03.11.2022 17:17:18	03.11.2022	
2	[redacted]	Antrag gestellt	07.11.2022 12:31:14	07.11.2022	Herrn [redacted] zur Prüfung vorgelegt.
3	[redacted]	Antrag gestellt	07.11.2022 15:23:01	07.11.2022	Die Beschwerde vom CCC dazu wird von [redacted] bearbeitet [redacted]. Da es um den gleichen Sachverhalt geht, schlage ich vor die Vorgänge zusammen zu bearbeiten. @[redacted] Ich kann das gerne übernehmen. Die Artikel 33-Meldung scheint schon weitere Informationen des Verantwortlichen zu enthalten. Viele Grüße [redacted]

4	[redacted]	abgeschlossen	11.11.2022 13:49:40	11.11.2022	Hinweise auf einen möglichen Datenabfluss scheint es nicht zu geben. Der Verantwortliche gibt außerdem an, die fehlerhafte Konfiguration behoben zu haben. Die vom CCC gemeldete IP-Adresse war eben auch nicht mehr erreichbar. Daher kann er Vorgang abgeschlossen werden. Viele Grüße [redacted]
5	[redacted]	Wiedervorlage	15.11.2022 11:13:07	09.12.2022	Aufgrund einer Beschwerde haben sich neue Anhaltspunkte ergeben.
6	[redacted]	Wiedervorlage	25.11.2022 07:17:00	25.11.2022	[redacted] vorgelegt.
7	[redacted]	abgeschlossen	25.11.2022 15:12:43	25.11.2022	Da es keine weiteren Anhaltspunkte auf einen unberechtigten Zugriff gibt, die Betroffenen aber dennoch informiert wurden, kann der Vorgang abgeschlossen werden. Den Petenten aus der Beschwerde werde ich ebenfalls informieren. Viele Grüße [redacted]

4. Bearbeitungshinweise

Hinweis von	[redacted]
Hinweisdatum	15.11.2022 07:34:06
Hinweis	Beschwerde liegt vor: T5.1.1-[redacted]

#	Hinweis von	Hinweisdatum	Hinweis
[redacted]			

5. Korrespondenzen

Art	Abschlussbescheid
Datum	25.11.2022 15:12:49
Bearbeiter	[redacted]
Text	Sehr geehrte[redacted] vielen Dank für Ihre Meldung vom 3.11.2022 und Ihre Stellungnahme vom 23.11.2022. Ich betrachte den Vorgang - vorbehaltlich neuer Erkenntnisse zum Sachverhalt - in meiner Zuständigkeit als abgeschlossen.
Anlage	
Text editieren	☒

#	Art	Datum	Bearbeiter	Text
1	Eingangsbestätigun	03.11.2022	[redacted]	Sehr geehrte/r Herr/Frau[redacted] Ihre Meldung vom 3.11.2022 ist bei uns eingegangen und wird unter dem Aktenzeichen T5.4-41480/22 bearbeitet. Bitte geben Sie das o. g. Aktenzeichen bei einer ergänzenden Meldung zum Vorfall und jedem weiteren Schriftverkehr mit unserer Dienststelle an.

2	Abschlussbescheid	11.11.2022	[redacted]	Sehr geehrte[redacted] vielen Dank für Ihre Meldung vom 3.11.2022. Ich betrachte den Vorgang - vorbehaltlich neuer Erkenntnisse zum Sachverhalt - in meiner Zuständigkeit als abgeschlossen.

3	Auskunft	15.11.2022	[redacted]	Sehr geehrte[redacted] vielen Dank für Ihre Meldung vom 3.11.2022. Bezüglich Ihrer Meldung fordere ich Sie unter Bezugnahme auf Art. 58 Abs. 1 lit. a DS-GVO auf, mir folgende Informationen mitzuteilen: Sie geben in der Meldung an, dass es keine Hinweise auf unberechtigte Zugriffe auf die Datenbank gibt. Mir liegt eine Beschwerde in diesem Zusammenhang vor, die Hinweise darauf enthält, dass die Datenbank bereits am 25.10.2022 von einer Suchmaschine indiziert wurde. Dabei wurde unter anderem offen gelegt, dass 670GB an Daten betroffen sind. Diese Indizierung erfolgte bereits vor dem ersten Zugriff durch den Chaos Computer Club, welcher Anfang November erfolgt ist. Ich bitte daher um erneute Überprüfung der Log-Dateien auf mögliche unberechtigte Zugriffe und eventuelle Datenabflüsse, sowie einen Bericht über die Ergebnisse der Auswertung. Damit die betroffenen Personen für möglicherweise folgende Angriffe und Betrugsmaschen sensibilisiert sind und ggf. in ihrer eigenen Sphäre Maßnahmen treffen können, empfehle ich – unabhängig vom Vorliegen einer Benachrichtigungspflicht nach Art. 34 DS-GVO –, die betroffenen Personen über den Vorfall zu informieren, wenn sich die Hinweise auf einen unberechtigten Zugriff bestätigen. Dies stellt in der Regel eine angemessene und geeignete Maßnahme zur Abmilderung möglicher nachteiliger Auswirkungen der Verletzung des Schutzes personenbezogener Daten im Sinne des Art. 33 Abs. 3 lit. d DS-GVO dar. Dies gilt insbesondere für die Personen, deren Bankdaten möglicherweise von den Angreifern abgegriffen wurden. Diese Information sollte insbesondere die möglichen Folgen für die betroffenen Personen beschreiben, für diese sensibilisieren und möglichst Empfehlungen für Schutzmaßnahmen, die die betroffenen Personen in ihrer eigenen Sphäre treffen können, umfassen. Für den Eingang Ihrer Stellungnahme habe ich mir eine Frist bis zum 9.12.2022 vorgemerkt.

4	Stellungnahme	23.11.2022	[redacted]	Von: [redacted]@acardo.com> Gesendet: Mittwoch, 23. November 2022 18:42 An: ZF LDI Referat-T (LDI) <Referat-T@ldi.nrw.de> Cc: [redacted] Betreff: AW: Ihre Meldung nach Art. 33 DS-GVO vom 3.11.2022 Sehr geehrte[redacted] vielen Dank für Ihre Rückfragen, die ich gerne beantworte: Wir haben die Logfiles und Statistiken intensiv ausgewertet, konnten aber bis auf den 2.11., also zu dem Zeitpunkt, zu dem der CCC zugegriffen hat, keine ungewöhnlichen Aktivitäten feststellen. Eine Meldung vor dem 2.11. liegt mir nicht vor. Den Bericht der Auswertung füge ich bei. Wir sind Ihrer Empfehlung gefolgt, die betroffenen Nutzer zu informieren. Eine Kopie der E-Mail finden Sie ebenfalls im Anhang. Für weitere Rückfragen und Auskünfte stehe ich Ihnen jederzeit gerne zur Verfügung. Viele Grüße [redacted] -- acardo group ag [redacted] Vorstand Am Kai 12, 44263 Dortmund, Germany
5	Abschlussbescheid	25.11.2022	[redacted]	Sehr geehrte[redacted] vielen Dank für Ihre Meldung vom 3.11.2022 und Ihre Stellungnahme vom 23.11.2022. Ich betrachte den Vorgang - vorbehaltlich neuer Erkenntnisse zum Sachverhalt - in meiner Zuständigkeit als abgeschlossen.

6. Aufgreifen eines Datenschutzverstoßes

Aufgreifendes Referat	
Rückmeldung erhalten am	
Aktenzeichen	
Maßnahmen nach Art. 58 Abs. 2	-
Bemerkungen	

7. IMI Eintragung

Datum	
IMI Case ID	
Bemerkungen	

Betreff: Wichtige Information zum Datenschutz
Datum: Mittwoch, 23. November 2022 um 16:16:31 Mitteleuropäische Normalzeit
Von: Dein couponplatz-Team
An: [redacted]

Liebe/r couponplatz-Nutzer/in,

wir sind stets darauf bedacht, unsere IT-Systeme auf dem aktuellen Stand zu halten. Datenschutz und Datensicherheit sind für uns nicht nur leere Worte, sondern haben für uns einen hohen Stellenwert. Umso mehr bedauern wir es, dass einem externen Sicherheitsforscher Anfang November aufgefallen ist, dass unsere Datenbank nicht vollständig gegen den Zugriff unberechtigter Dritter abgesichert war.

Selbstverständlich haben wir diese Schwachstelle binnen weniger Minuten nach Kenntniserlangung geschlossen und weitere technische Maßnahmen ergriffen, um unsere Systeme noch besser abzusichern und solche Vorfälle künftig zu vermeiden.

Obwohl uns keinerlei Hinweise darauf vorliegen, dass unbekannte Dritte Zugriff auf Teile unserer Datenbank und gegen unseren Willen möglicherweise Einblick in personenbezogene Daten unserer Nutzer gehabt haben, möchten wir Dich hiermit aktiv hierüber informieren. Selbstverständlich haben wir vorsorglich auch die zuständige Datenschutzbehörde informiert.

Da wir nicht zu 100% ausschließen können, dass unbekannte Dritte Zugriff auf

Deine Daten hatten, besteht theoretisch das Risiko, dass Du Opfer eines Betrugs oder Identitätsdiebstahls werden könntest. Wir empfehlen Dir daher, künftig auf verdächtige Vorkommnisse zu achten.

Für eventuelle Rückfragen stehen wir Dir gerne unter sicherheit@couponplatz.de zur Verfügung.

Dein couponplatz-Team

Wenn Du Dich nicht registriert hast, bitten wir die E-Mail zu ignorieren und entschuldigen uns.

Am Kai 12 - 44263 Dortmund - Deutschland

Gesetzliche Vertretungsberechtigte:
Geschäftsführer Robert Hartung, Constantin Rack, Christoph Thye

Kontakt
E-Mail: support@couponplatz.de | Web: couponplatz.de

Handelsregistereintragung
Amtsgericht Dortmund HRB 29362 | Ust-Id-Nr.: DE313092261

2022-11-03 Security Incident

Summary

One of our databases was publicly accessible with the default user from 2022-09-19 until 2022-11-03.

Timeline

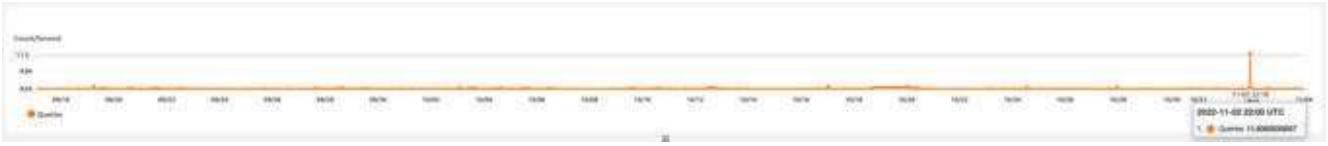
2022-09-19 14:07

A default database user was created accidentially

2022-11-02 23:47

The Chaos Computer Club Member [redacted] informed us by mail to info@acardo.com with [redacted]ccc.de in copy about the security leak.

As it's mentioned in the screenshot below there was a high load **only** in 2022-11-02 at 22:00 UTC (23:00 German time UTC+1)



To confirm the time also the connection was done by CCC here is error log of a login attempt by user '[redacted]' which is in the list of cc in Chaos Computer Club mail ([redacted]ccc.de)

```
2022-11-02T21:50:00.426105Z 143183 [Note] Aborted connection 143183 to db: 'scondoo-production' user: [redacted] host: '193.96.224.75'
(Got an error writing communication packets)
2022-11-02T21:52:40.899644Z 143197 [Note] Aborted connection 143197 to db: 'migration_scondoo_api' user: [redacted] host:
'193.96.224.75' (Got an error writing communication packets)
---------------------- END OF LOG ----------------------
```

as shown in the logs the timeframe is quite the same with the high load.

2022-11-03 14:14

Mail was forwarded to [redacted]

2022-11-03 14:29

Default user was deleted by [redacted] and we informed the Chaos Computer Club informed about.

2022-11-03 17:17

We informed the Landesamt für Datenschutz und Informationssicherheit NRW about the security leak.

2022-11-23 16:00

We informed the affected users about the security leak:

> ***Betreff: Wichtige Information zum Datenschutz***
>
> *Liebe/r couponplatz-Nutzer/in,*
>
> *wir sind stets darauf bedacht, unsere IT-Systeme auf dem aktuellen Stand zu halten. Datenschutz und Datensicherheit sind für uns nicht nur leere Worte, sondern haben für uns einen hohen Stellenwert. Umso mehr bedauern wir es, dass es einem externen Sicherheitsforscher Anfang November aufgefallen ist, dass unsere Datenbank nicht vollständig gegen den Zugriff unberechtigter Dritter abgesichert war.*
>
> *Selbstverständlich haben wir diese Schwachstelle binnen weniger Minuten nach Kenntniserlangung geschlossen und weitere technische Maßnahmen ergriffen, um unsere Systeme noch besser abzusichern und solche Vorfälle künftig zu vermeiden.*
>
> *Obwohl uns keinerlei Hinweise darauf vorliegen, dass unbekannte Dritte Zugriff auf Teile unserer Datenbank und gegen unseren Willen möglicherweise Einblick in personenbezogene Daten unserer Nutzer gehabt haben, möchten wir Dich hiermit aktiv hierüber informieren. Selbstverständlich haben wir vorsorglich auch die zuständige Datenschutzbehörde informiert.*

Da wir nicht zu 100% ausschließen können, dass unbekannte Dritte Zugriff auf Deine Daten hatten, besteht theoretisch das Risiko, dass Du Opfer eines Betrugs oder Identitätsdiebstahls werden könntest. Wir empfehlen Dir daher, künftig auf verdächtige Vorkommnisse zu achten.

Für eventuelle Rückfragen stehen wir Dir gerne unter sicherheit@couponplatz.de zur Verfügung.

Dein couponplatz-Team