RE: Potentiala bresa RGPD - Divulgare date cu caracter personal in cererile WEB

dpo@daikokuten.ro
To: office@incorpo.ro

September 7, 2023 at 5:08 PM

Bună ziua

Vă mulțumim pentru informare

Vom lua măsurile de rigoare

Cu stimă,

Pavel HALMAGEAN - DPO

From: office@incorpo.ro <office@incorpo.ro>
Sent: Thursday, September 7, 2023 09:56
To: dpo@ceccar.ro; contact@ceccar.ro
Subject: Potentiala bresa RGPD - Divulgare date cu caracter personal in cererile WEB

Buna ziua,

.

Va contactez in legatura cu o potentiala bresa a Regulamentului General de Protectie a Datelor cu Caracter Personal, prin divulgarea neintentionata a unui numar semnificativ de date cu caracter personal, printre care:

- Nume si Prenume
- CNP (Si datele direct incluse in acesta)
- Adresa (Fie a biroului, fie domiciliu)
- Data si locul nasterii (inclusiv localitate)
- Numere de telefon mobil (si un unele situatii, fix)
- Adresa postala (diferita de adresa)
- Date referitoare la inregistrarea in tabloul CECCAR (Aceste informatii sunt insa intentionate a fi afisate, in opinia naostra)
- CIP
- **Cetatenia** (Posibil sa se incadreze in categoria de date cu caracter personal sensibile, identificand etnia persoanelor)

Exemplu date cu caracter personal


```
{
 "uuid": "UUID (DIN SERVER PROBABIL)",
 "appCeccarId": 0,
 "showPersonalInfo": true,
 "firstName": "Prenume",
 "lastName": "Nume",
 "fullName": "Nume Intreg",
 "cnp": "CNP",
 "sex": "Sex (1 sau 2)",
 "birthDate": "Data nasterii - ZZ.LL.AAAA",
 "birthPlace": "Locul si Judetul nasterii",
 "address": "Adresa de domiciliu, posibil sediu declarat",
 "mailAddress": "Adresa postala",
 "phoneNumber": "Numar de telefon",
 "mobileNumber": "Numar de telefon Mobil",
```

"emailAddress": "Email declarat",

"web": "Site web declarat",

"apea": "APEA",

"authorizationNumber": "Numar autorizatie",

"region": {

"id": 0,

"code": "JUDET (COD)",

"name": "JUDET (NUME)"

},

"professionalCategory": {

"id": 2,

"code": "Categorie Profesionala cod",

"name": "Categorie Profesionala (Nume)"

},

"professionalCategory2": null,

"professionalCategory3": null,

"regNumber": "Numar inregistrare (probabil in tabel)",

"promotionYear": null,

"monitorCategory": {

"id": 0,

"code": "Categorie Monitor (CoD)",

"name": "Categorie Monitor (Nume)"

},

"citizenship": "Cetatenie - Poate reprezenta o data cu caracter personal sensibila (Etnia)",

"newBookReleaseDate": "(Data \"New Book?\")",

"bookChanged": false,

"bookChangedDate": "1970-01-01",

"joinYear": "Data intrare in profesie",

"internshipYear": 0,

"internshipType": "",

"internshipExamAccess": 0,

"internshipCertificateNumber": "",

"internshipBecomeType": "0",

"internshipTest": "0",

"internshipCafr": false,

"internshipReportsTotalNumber": 0,

"internshipDate": null,

"internshipBecomeDate": "Data definitivat",

"internshipCollegeGraduate": "",

"internshipComments": "",

"cip": "CIP",

"memberType": null,

"currentYearVisa": "1 sau 0 (are viza pt lucrat curent). Inclusiv persoane radiate au datele divulgate. Este posibil ca persoanele radiate sa trebuiasca, conform pr incipiilor GDPR, eliminate din baza de date."

}

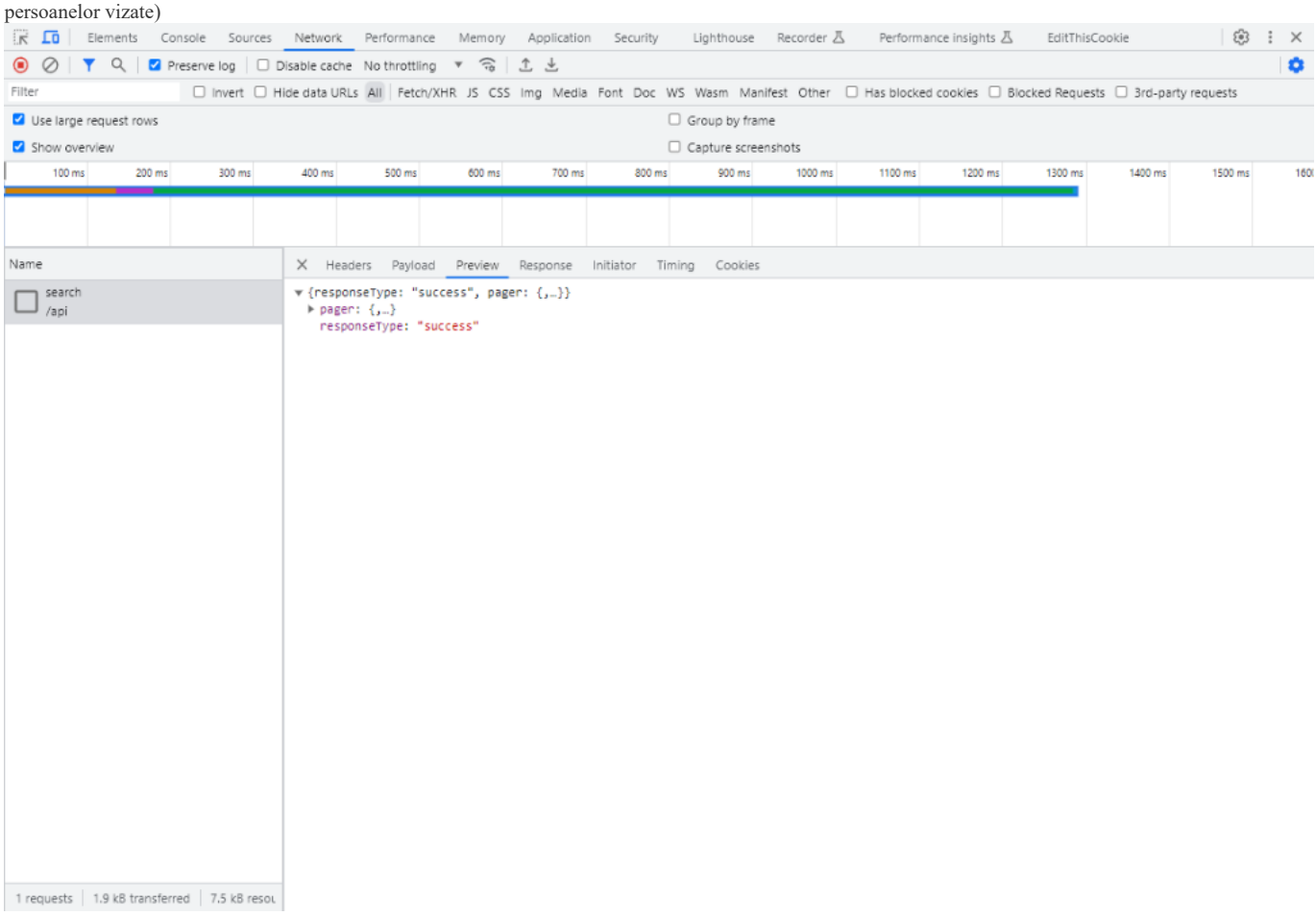
Privitor la bresa, sunt vizate peste 50.000 persoane fizice, a caror date cu caracter personal au fost divulgate, in opinia noastra. Nu cunoastem data aparitiei initiale a bresei, dar o corelam cu implementarea sistemului de raportare nou, accesibil la https://raportare.ceccar.ro/search.

In mod normal, in momentul efectuarii unui request WEB pentru obtinerea unor informatii, pentru a fi afisate, serverul WEB transmite doar informatiile necesare spre a se furniza, si nu totalitatea informatiilor existente pe baza de date a procesatorului de date.

In caz contrar, chiar daca aplicatia nu afiseaza in mod implicit informatiile, acestea se pot citi extrem de usor, inclusiv fara prezenta unor cunostinte tehnice.

- **Prin utilizarea functiei de "Inspect"**, furnizata de browserele Chromium (Chrome, Edge, etc) sau analoagele acestora, pe alte platforme web (Safari, Firefox), prin vizualizarea request-urilor (cererilor) si raspunsurilor date de serverul gestionat de CECCAR.

  Pentru a testa vulnerabilitatea:

1. Se intra pe site-ul CECCAR de cautare (https://raportare.ceccar.ro/search)
2. Se da click dreapta pe ecran, se apasa "Inspect"
3. Se selecteaza casuta network, si se face orice cautare pe tablou
4. Datele sensibile apar in sectiunea "Response", a cererii web efectuate. (Nu s-a afisat sectiunea Response, fiind de natura sa afiseze datele sensibile ale persoanelor vizate)
5. 

- **Prin utilizarea unui proxy intermediar**, sau prin transmiterea manuala a request-urilor, situatie in care se poate accesa, secvential, totalitatea contabililor, si implicit, obtinerea datelor cu acces personal a tuturor acestora.

Riscuri si mentiuni suplimentare

In opinia noastra, efortul minim de accesare a datelor respective, impreuna cu faptul ca datele sunt in mod neechivoc sensibile, care pot duce inclusiv la furtul de identitate sau uzurparea calitatii de expert contabil sau contabil autorizat a membrilor CECCAR, reprezinta o problema care necesita solutionata.

Desi nu putem amplasa in timp cu exactitate aparitia acestor informatii "in the wild" - adica, cand au inceput a putut fi accesate public, de catre oricine, opinam ca cel mai probabil, si alti actori, maliciosi sau nu, au inceput analizarea datelor.

Este notabil ca anumite platforme de tip motor de cautare, precum Shodan, sau browsere web mai complexe, indexeaza in mod implicit platformele web fara o politica robots.txt restrictiva. Or, indexarea in motoare de cautare accesibile public a CNP-urilor, numelor intregi, adreselor, etc a persoanelor reprezinta un risc semnificativ si care afecteaza in mod direct beneficiarii si membrii CECCAR.

Va stam la dispozitie, in mod gratuit, cu consultanta si asistenta pentru solutionarea probemelor, precum si pentru detalii pentru identificarea si reproducerea vulnerabilitatii, la adresa telefonica si numarul de telefon prezentat *infra.*

Cu stima,

Image removed by sender. Incorpo.Ro Logo

Deleanu Stefan-Lucian
Director / ENTRYRISE S.R.L

Website: www.incorpo.ro
Email: office@incorpo.ro
Phone: +40786833325