



Claude WISELER
President vun der
Chamber vun den Deputéierten
19, um Krautmaat
L-1728 Lëtzebuerg

Lëtzebuerg, den 29/07/2026

Här President,

Sou wéi den Artikel 80 vun eisem Chambersreglement et virgesäit, bieden ech lech, dës parlamentaresch Fro un d'Ministère fir den Interieur, Bildung, Kanner a Jugend & Famill, Solidaritéit an Integratioun weiderzeleeden.

De 16. Juli 2026 ass d'asbl Arcus – Kanner, Jugend a Famill Affer vun engem Cyberattack ginn. An engem Communiqué vum 24. Juli 2026 huet d'Organisatioun confirméiert, datt en onbefugten Drëtten Zougrëff op Donnéeën op hire Systemer hat, an datt et no den aktuellen techneschen Analyse warscheinlech ass, datt en Deel vun dësen Donnéeën exfiltréiert gouf. D'Aarbechten, fir feststellen, wéi eng Fichieren a wéi eng Persounen betraff sinn, lafe weider.

Arcus ass ee vun de gréisste konventionéierten Träger am sozialen an educative Beräich a betreit ënner anerem Crèchen, Foyeren, Internater a Berodungsdéngschter. Et geet domat potenziell ëm héichsensibel Donnéeën vu Kanner, Jugendlechen a Familljen: psychosozial Informatiounen, Identitéits- a Finanzdonnéeën, an eventuell och Donnéeën, déi ënnert den Artikel 9 vum RGPD falen. Bei Kanner, déi am Kader vun enger Kannerschutzmoossnam placéiert sinn, kann d'Bekanntginn vun Adressen oder Plazéierungsinformatiounen doriwwer eraus eng konkret Gefor fir hir kierperlech Sécherheet duerstellen.

Iwwert dëse konkrete Fall eraus stellt sech d'Fro, wéi eng Ufuerderungen de Staat de konventionéierten Träger am Beräich vun der Cybersécherheet iwwerhaapt stellt, wann hien hinnen d'Betreiung vun deene vulnerabelste vum Land uvertraut.

An deem Zesummenhang wëllt ech de Ministeren dës Froe stellen:

1. Wéini a wéi sinn déi zoustänneg Ministèren iwwer den Incident informéiert ginn?
2. Ass d'Nationale Kommissioun fir den Dateschutz (CNPd) am Delai vun 72 Stonnen notifiéiert ginn?



3. Sinn den HCPN respektiv GOVCERT.LU agebonne ginn? Huet den Träger staatlech Ënnerstëtzung ugefrot – a wa jo, wéi eng gouf geleeest?
4. Ass eng Plainte bei de Sécherheetsautoritéite gemaach ginn?
5. Verfüügt d'Regierung iwwer Informatiounen zur Zuel vun de betraffene Persounen a zu de Kategorie vun Donnéeën, notamment souguer Donnéeën am Sënn vum Artikel 9 RGPD? Wéi vill Mineure sinn dorënner?
6. Sinn déi betraffene Persounen individuell informéiert ginn (Art. 34 RGPD)? Wéi ginn ehemoleg Usagere respektiv hir legal Vertrieeder erreecht?
7. Ass gepréift ginn, ob Donnéeën iwwer Plazéierungen (Adressen, Moosnamen am Kader vum Kannerschutz) betraff sinn – a wa jo, wéi eng Schutzmoosname ginn en faveur vun deene Kanner geholl?
8. Wéi eng konkret Ënnerstëtzung (Hotline, juristesche Begleedung, Suivi bei Identitéitsmëssbrauch) kréien déi betraffene Familljen, a wien iwwerhëlt d'Käschten dofir?
9. Wéi eng Cybersecherheets Measure hat Arcus am Asaz fir den den Impakt vun der Fuite vun Donnéeën ze minimiséieren (Verschlësslung vu sensibelen Daten, Need to Know, Least Privilege....)?
10. Wéi eng konkret Cybersécherheetsufuerderunge gesinn d'Konventiounen tëscht dem Staat an den Träger vir, iwwert en allgemenge Passus zum RGPD eraus?
11. Ginn et Mindeststandarden (z. B. ISO 27001 oder equivalent), obligatoresch extern Auditen oder Sécherheetstester? Wa nee, firwat net?
12. Fälen Träger vun der Gréisst vun Arcus ënnert den Uwendungsberäich vum NIS2-Kader? Wa nee, gedenkt d'Regierung de Perimeter unzepassen?
13. Musse d'Träger nowiesen, datt déi zur Verfügung gestallte staatlech Mëttel och effektiv an d'IT-Sécherheet an RGPD Konformitéit investéiert ginn? Gëtt dat kontrolléiert – a vu wem?
14. Wéi eng legislativ oder reglementaresch Initiative sinn zanter der Caritas-Affär geholl ginn, fir d'Gouvernancefunktione (intern Kontroll, Risikomanagement, Auditfunktione) bei de konventionéierten Träger ze professionaliséieren?
15. Wéi vill Cyberincidenter goufen an de leschte fënnef Joer vun Träger am sozialen an educative Beräich un d'Ministèren oder un d'CNPD gemellt?

16. Gedenkt d'Regierung e mutualiséierten IT- a Sécherheetsdéngscht fir de Secteur opzebauen (z. B. e gemeinsamen SOC, Ënnerstëtzung duerch de CTIE, oder Kaderkontrakter fir Audite), fir datt kleng a mëttel Träger net eleng dostinn?
17. Ass virgesinn, d'Dauer vun der Konservatioun vun de Donnéeën am Secteur ze reglementéieren, fir d'Volume vun histoireschen Donnéeën ze reduzéieren?

Mat déiwem Respekt,



CLEMENT Sven
Deputéierten





Gemeinsam Äntwert vum Minister fir Educatioun, Kanner a Jugend, Claude Meisch, a vum Minister fir Famill, Solidaritéit, Zesummeliwwen an Accueil, Max Hahn, op d'parlamentaresch Fro Nr. 4554 vum honorabelen Deputéierte Sven Clement

1. Wéini a wéi sinn déi zoustänneg Ministèrenen iwwer den Incident informéiert ginn?

Den Dag selwer, wou d'Attack identifizéiert ginn ass (d. h. den 16. Juli 2026), huet ARCUS (dono „de concernéierte Gestionnaire“) de Ministère fir Educatioun, Kanner a Jugend (dono „Ministère“) informéiert; d'Kommunikatioun ass de 16. Juli prioritär iwwer Telefon verlaf.

Den 18. Juli huet de concernéierte Gestionnaire de Ministère mat weideren Detailen schrëftlech informéiert.

2. Ass d'Nationale Kommissioun fir den Dadeschutz (CNPD) am Delai vun 72 Stonnen notifiéiert ginn?

Jo, de concernéierte Gestionnaire huet d'CNPD am Delai vun 72 Stonnen notifiéiert (de 17. Juli 2026).

3. Sinn den HCPN respektiv GOVCERT.LU agebonne ginn? Huet den Träger staatlech Ënnerstëtzung ugefrot – a wa jo, wéi eng gouf geleeest?

4. Ass eng Plainte bei de Sécherheetsautoritéite gemaach ginn?

Op Basis vun den Informatiounen, déi eis zur Verfügung gestallt goufen, huet de concernéierte Gestionnaire de 16. Juli mat den ënnerschiddlechen staatlechen Autoritéite Kontakt opgeholl. Direkt Ënnerstëtzung krut de concernéierte Gestionnaire vun der Unité Cybercrime vun der Police judiciaire a vum *Computer Incident Response Center Luxembourg* (CIRCL).

Duerch dës Gespréicher huet de concernéierte Gestionnaire engersäits déi entspriechend Instanzen informéiert iwwer de jeeweilege Wëssensstand; gläichzäiteg ass de concernéierte Gestionnaire vun de staatlechen Autoritéite berode ginn iwwer déi richteg extern Ënnerstëtzung an déi noutwennege Aktiounen/Reaktiounen:

- de GOVCERT (16.7., Verweis un de CIRCL, well de GOVCERT zoustänneg fir Cyberattacken op staatlech Unitéiten an Établissements publics ass);
- de CIRCL (16.07., 14:00 Auer), iwwer Telefon;
- d'Unité Cybercrime (16.7.) vun der Police judiciaire;
- den HCPN ass de 17. Juli per Telefon kontaktéiert ginn; si sinn awer fir de concernéierte Gestionnaire net zoustänneg (Sécherheet fir strukturelevant Institutiounen; si ginn nëmmen aktiv, wann een op hirer Lëscht steet).

Doriwwer eraus ass de Ministère informéiert ginn, datt de concernéierte Gestionnaire den 16. Juli extern Spezialiste fir Cybersecurity engagéiert huet, fir par rapport zum Schutz vun den Donnéeën an

der Widderhierstellung vun der IT-Infrastruktur déi néideg Ënnerstëtzung ze kréien a virun allem fir forensesch IT-Analysen no der Attack auszuféieren.

5. Verfüügt d'Regierung iwwer Informatiounen zur Zuel vun de betraffene Persounen a zu de Kategorie vun Donnéeën, notament souguer Donnéeën am Sënn vum Artikel 9 RGPD? Wéi vill Mineure sinn dorënner?

Laut den Informatiounen, déi dem Ministère virleien, goufen déi néideg Schrëtter an d'Weeër geleet an déi zoustänneg Instanzen informéiert.

6. Sinn déi betraffene Persounen individuell informéiert ginn (Art. 34 RGPD)? Wéi ginn ehemoleg Usagere respektiv hir legal Vertrieder erreecht?

Jo, déi betraffene Persounen sinn individuell informéiert ginn. An deem Kontext mussen zwee verschidden Zäitraim gekuckt ginn:

1) Direkt no der Attack:

De concernéierte Gestionnaire huet am Kader vun deem, wat de 16. an de 17. Juli u Kommunikatiounsmëttelen zur Verfügung stoung, de Maximum u Kontakt opgehol mat:

- De Chargés de Direction/Chefs de service vun de Strukturen duerch Reuniounen a Workshops en présentiel
- Déi Responsabel hunn de Message an hire respektive Servicier un d'Mataarbechter vun de concernéierte Gestionnaire viruginn.
- De concernéierte Gestionnaire huet de 17. Juli d'Ëffentlechkeet informéiert. Deen Dag ass en éischte Communiqué de presse un all déi relevant Medienhaiser vum Land erausgeschéckt ginn.
- D'Adressdatebanke vun de Clientë stoungen do nach net zur Verfügung, esou datt zu deem Zäitpunkt eng méi cibléiert Kommunikatioun net méiglech war.

2) Direkt d'Woch drop (20.-27. Juli):

Nodeems duerch d'analytesch Aarbecht vum 16. bis den 19. Juli kloer war, datt de concernéierte Gestionnaire Affer vun enger Cyberattack ginn ass, an datt d'Exfiltratioun vun Donnéeën méiglech war, huet de concernéierte Gestionnaire preventiv d'Clienten informéiert. Inhalt vun der Informatioun waren déi potentiell Risiken, den Opruff, virsiichteg ze sinn, esouwéi Hëllefstellung fir d'Clienten, wat si preventiv kéinte maachen:

- mat Deplianten an Informatiounsbréiwer am direkte Kontakt;
- mat Affichen an allen Strukturen;
- um Internetsite vum concernéierte Gestionnaire iwwert e FAQ;
- iwwer eng Hotline, op där all potentiell betraffene Persoun uruffe kann, fir direkt Berodung ze kréien (+352 283802). D'Nummer vun der Hotline ass iwwer d'Affichen, d'Deplianten a Bréiwer esouwéi FAQe fir d'Clienten a fir d'Mataarbechter vum concernéierte Gestionnaire bekannt gemaach ginn.

Duerch d'Aarbecht vun den externen Experte konnt de concernéierte Gestionnaire en zweeten, vill méi détailléierte Communiqué de presse redigéieren, deen de 24. Juli un déi national Medienhaier verschéckt ginn ass.

De concernéierte Gestionnaire huet d'Mataarbechter iwwer en individuelle Bréif informéiert, an am Intranet e FAQ fir si publizéiert. D'Hotline ass och fir d'Mataarbechter vum concernéierte Gestionnaire zougänglech.

Eemoleg Clienten huet de concernéierten Gestionnaire informéiert iwwer d'Press, iwwer FAQen um Internetsite esouwéi iwwer d'Hotline.

7. Ass gepréift ginn, ob Donnéeën iwwer Plazéierungen (Adressen, Moosnamen am Kader vum Kannerschutz) betraff sinn – a wa jo, wéi eng Schutzmoosname ginn en faveur vun deene Kanner geholl?

Dem Ministère leien aktuell keng Informatiounen vir, déi drop hindeiten, datt Donnéeën iwwer Plazéierungen oder spezifesch Moosnamen am Kader vum Kannerschutz betraff sinn. De Ministère steet an enkem Kontakt mam Gestionnaire a suivéiert d'Situatioun ganz genee. Laut den Informatiounen vum Gestionnaire huet dësen déi néideg Moosnamen ergraff, fir potenziell betraffe Persounen ze informéieren.

8. Wéi eng konkret Ënnerstëtzung (Hotline, juristesche Begleedung, Suivi bei Identitéitsmëssbrauch) kréien déi betraffe Familljen, a wien iwwerhëlt d'Käschten dofir?

De Ministère verweist op d'Äntwert vun der Fro Nr. 6.

9. Wéi eng Cybersecherheets Measure hat ARCUS am Asaz fir den Impakt vun der Fuite vun Donnéeën ze minimiséieren (Verschlësslung vu sensibelen Daten, Need to Know, Least Privilege....)?

Laut den Informatiounen, déi dem Ministère virleien, hat de concernéierte Gestionnaire zum Zäitpunkt vum Virfall eng breet Pallett vu Cybersécherheetsmesuren am Asaz, dorënner Verschlësslungsléisungen, eng Benotzer- a Rechterverwaltung op Basis vun „Need-to-Know“- a „Least-Privilege“-Prinzipien, an Authentifikatiouns- a Zougangskontrollen.

10. Wéi en konkret Cybersécherheetsufuerderunge gesinn d'Konventiounen tëscht dem Staat an den Träger vir, iwwer en allgemenge Passus zum RGPD eraus?

Wat d'Cybersécherheetsufuerderungen ugeet, gesinn d'Konventiounen, déi vum Ministère mat den Träger ofgeschloss ginn, aktuell keng spezifesch technesch oder organisatoresch Ufuerderungen am Beräich vun der Cybersécherheet vir, déi iwwer en allgemenge Passus vum RGPD erausginn.

11. Ginn et Mindeststandarden (z. B. ISO 27001 oder equivalent), obligatoresch extern Auditen oder Sécherheetstester? Wa nee, firwat net?

Dës Fro reit sech an déi méi breet Aarbechten zur Weiderentwécklung vum konventionelle Kader an. Am Kader vum Protocole d'entente ass virgesinn, d'Conditions générales an déi weider Virgaben am géigesäitegen Accord mam Secteur auszeschaffen. An deem Zesummenhang kënnen och d'Ufuerderungen am Beräich vun der Datasécherheet an der Cybersécherheet behandelt ginn, fir gemeinsam Léisungen ze entwéckelen, déi un d'Realitéit vum Secteur ugepasst sinn.

12. Fallen Träger vun der Gréisst vun ARCUS ënnert den Uwendungsberäich vum NIS2-Kader? Wa nee, gedenkt d'Regierung de Perimeter unzepassen?

De concernéierte Gestionnaire fällt net direkt ënnert NIS2, well si a kee vun den annexéierte Secteure falen. D'Gréisst vum concernéierte Gestionnaire spillt dobäi keng Roll.

Et gëtt aktuell en internen Aarbechtsgrupp fir de Staat, deen sech mam Uwendungsberäich am Perimeter vun NIS2 beschäftegt.

13. Musse d'Träger nowiesen, datt déi zur Verfügung gestallte staatlech Mëttel och effektiv an d'IT-Sécherheet an RGPD Konformitéit investéiert ginn? Gëtt dat kontrolléiert – a vu wem?

Am Kader vun den ASFT-Konventionne sinn d'Träger verpflichtet, all Joer hir Decompten anzerechen, an deenen esouwuel d'Recetten ewéi och d'Depensen ausgewise ginn. Dës kënnen och Ausgabe betreffend den IT-Beräich enthalten. De Ministère ka bei Bedarf méi Detailler nofroen.

D'Verantwortung fir d'IT-Sécherheet an d'Konformitéit mat den Ufuerderungen am Beräich vum Dateschutz läit par contre beim jeeweilegen Träger.

14. Wéi eng legislativ oder reglementaresch Initiative sinn zanter der Caritas-Affär geholl ginn, fir d'Gouvernancefunktione (intern Kontroll, Risikomanagement, Auditfunktione) bei de konventionéierten Träger ze professionaliséieren?

Fir d'Gouvernancefunktione bei de konventionéierte Gestionnairen ze stäerken, setzt d'Regierung op déi gemeinsam Aarbechte mam Secteur am Kader vum Protocole d'entente mat der FEDAS. D'Aarbechtsgruppen iwwer Gouvernance, Finanzement a Kontroll bidden de Kader, fir och d'Froe vun der interner Kontroll, dem Risikomanagement an den Auditfunktione ze behandelen. Zil ass et, gemeinsam a praxisorientéiert Virgaben auszeschaffen an de konventionelle Kader deementspreechend weiderzeentwéckelen.

15. Wéi vill Cyberincidenter goufen an de leschte fënnef Joer vun Träger am sozialen an educative Beräich un d'Ministèren oder un d'CNPD gemellt?

Et sinn dem Ministère keng weider Cyberincidente gemellt ginn, och net vun anere konventionéierten Träger.

16. Gedenkt d'Regierung e mutualiséierten IT- a Sécherheidsdéngscht fir de Secteur opzebauen (z. B. e gemeinsamen SOC, Ënnerstëtzung duerch de CTIE, oder Kaderkontrakter fir Audite), fir datt kleng an mëttel Träger net eleng do stinn?

De Ministère ass sech bewusst, datt d'Ëmsetzung vun den Ufuerderungen am Beräich vum Dateschutz a vun der Cybersécherheet besonnesch fir kleng a mëttelgrouss Träger eng Erausforderung duerstelle kann.

An dësem Kontext gi schonn haut Formatiounen vu verschiddenen offiziellen Acteuren ugebueden. Doriwwer eraus ginn aktuell intern Reflexiounen gefouert, fir ze préiwen, ob an a wéi enger Form, zesumme mat externen Acteuren, spezifesche Formatiounen zu dësem Theme fir de Secteur kéinten ugebuede ginn.

17. Ass virgesinn, d'Dauer vun der Konservatioun vun de Donnéeën am Secteur ze reglementéieren, fir d'Volume vun historeschen Donnéeën ze reduzéieren?

D'Späicherfriste vun den Donnéeën am Secteur sinn am Aklang mam RGPD, dem uwendbaren Archivagekader an de spezifischen Dateschutzbestëmmunge vun de jeeweilege sektorielle Gesetzer festgeluecht. Zesumme mam Secteur gëtt gekuckt, wéi d'Gestionnaire bei der Ëmsetzung vun den uwendbare Virgaben ënnerstëtzt kënne ginn.

Lëtzebuerg, de 7. Oktober 2026

De Minister fir Educatioun,
Kanner a Jugend

(s.) Claude MEISCH