black hat® EUROPE 2023

DECEMBER 4-7

EXCEL LONDON / UK

JSIG

black hat EUROPE 2023

Illegitimate Data Protection Requests: To Delete or to Address?

Delivered by:

Mark Povey: Technical Director and Chief DPO at JS Information Governance Ltd
Larisa Munteanu: Data Protection Lawyer/DPO at JS Information Governance Ltd, PhD Researcher at Erasmus School of Law (Erasmus University Rotterdam)

JSIG

Privacy – where is the new oil?

Data as the key element

- European Parliament (2020) – "while oil is obviously a finite and non-reusable resource, data can be infinite and reused – with account taken of ownership and access rights"

Source: Is data the new oil? (europa.eu)

Relevance

- Evolution in the way individuals (even perpetrators) acknowledge the value of personal data
- Digitalisation and subsequently, cyber-crimes
- Legal requirements imposed on both public and private sector

International and Regional Legal Obligations

- Convention 108 GDPR
- NIS 2 Directive

National Legal Obligations

- Data Protection Act 2018
- Computer Misuse Act 1990 (UK)
- BSI Act (Germany)
- Organic Law 3/2018 (Spain)…

GDPR References

- Art. 5 (1) f) – integrity and confidentiality
- Art. 5 (2) – accountability of the General Data Protection Regulation

Operational Measures

- Friend or FOI?

Operational Measures

- Access restrictions – "least privilege" principle
- Incident response and disaster recovery plans

Operational Measures

- Encryption at rest and in transit
- Validate ID
- Prior verifications

Organisational Measures

- Clear roles and responsibilities throughout the organisation

Organisational Measures

- Solid framework supporting data security with policies and procedures
- ISO standard?

Organisational Measures

- Training and awareness

Data Protection by Design and by Default – Art. 25 GDPR

DP by Design

- must take into account risks and severity for "rights and freedoms of natural persons posed by the processing (…) **both at the time of the determination of the means for processing and at the time of the processing itself**"

DP by Default

- must "implement appropriate technical and organizational measures for ensuring that, **by default** only personal data which are necessary for each specific purpose of the processing are processed"

BlackHat USA 2019

James Pavur - “GDPArrrrr: Using Privacy Laws to Steal Identities” (2019)

Apparently valid requests, yet a legal omission
➡ Knowledge limitations and operational constraints

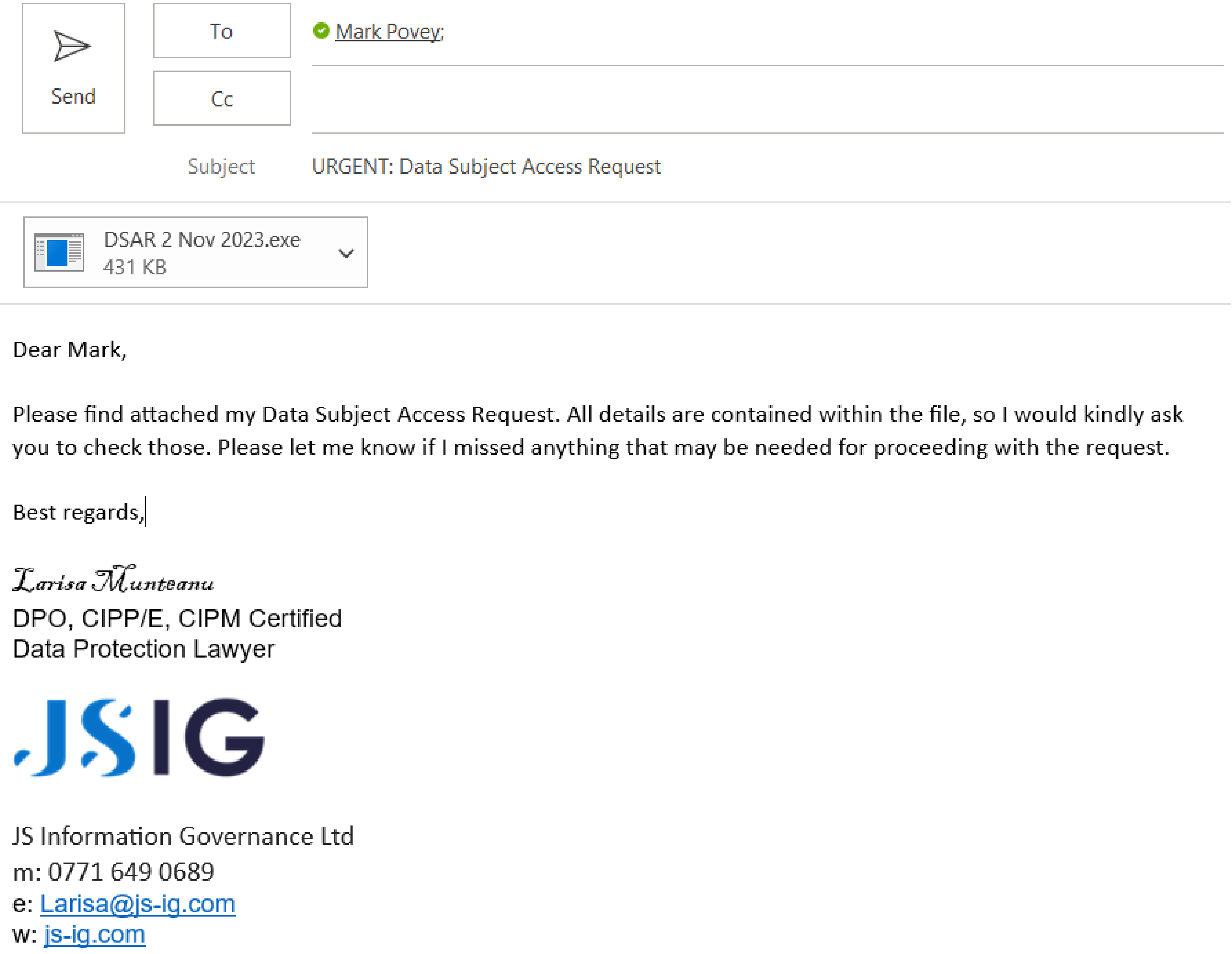
Manifestly unfounded/excessive:

“These reasons relate to malicious intent on the part of the sender but do not discuss the possibility of fraud directly - focusing instead on the abuse of GDPR requests to waste organizational resources”

Source: https://doi.org/10.48550/arXiv.1912.00731

Malware attack

- Data Subject Access Requests (DSARs) accompanied by a malware attack – you may get tricked by the name of the file
- The file extension is relevant too – although there are no legal restrictions on the format for such requests, you will definitely not receive it as an executable file



To: Mark Povey;

Subject: URGENT: Data Subject Access Request

DSAR 2 Nov 2023.exe
431 KB

Dear Mark,

Please find attached my Data Subject Access Request. All details are contained within the file, so I would kindly ask you to check those. Please let me know if I missed anything that may be needed for proceeding with the request.

Best regards,

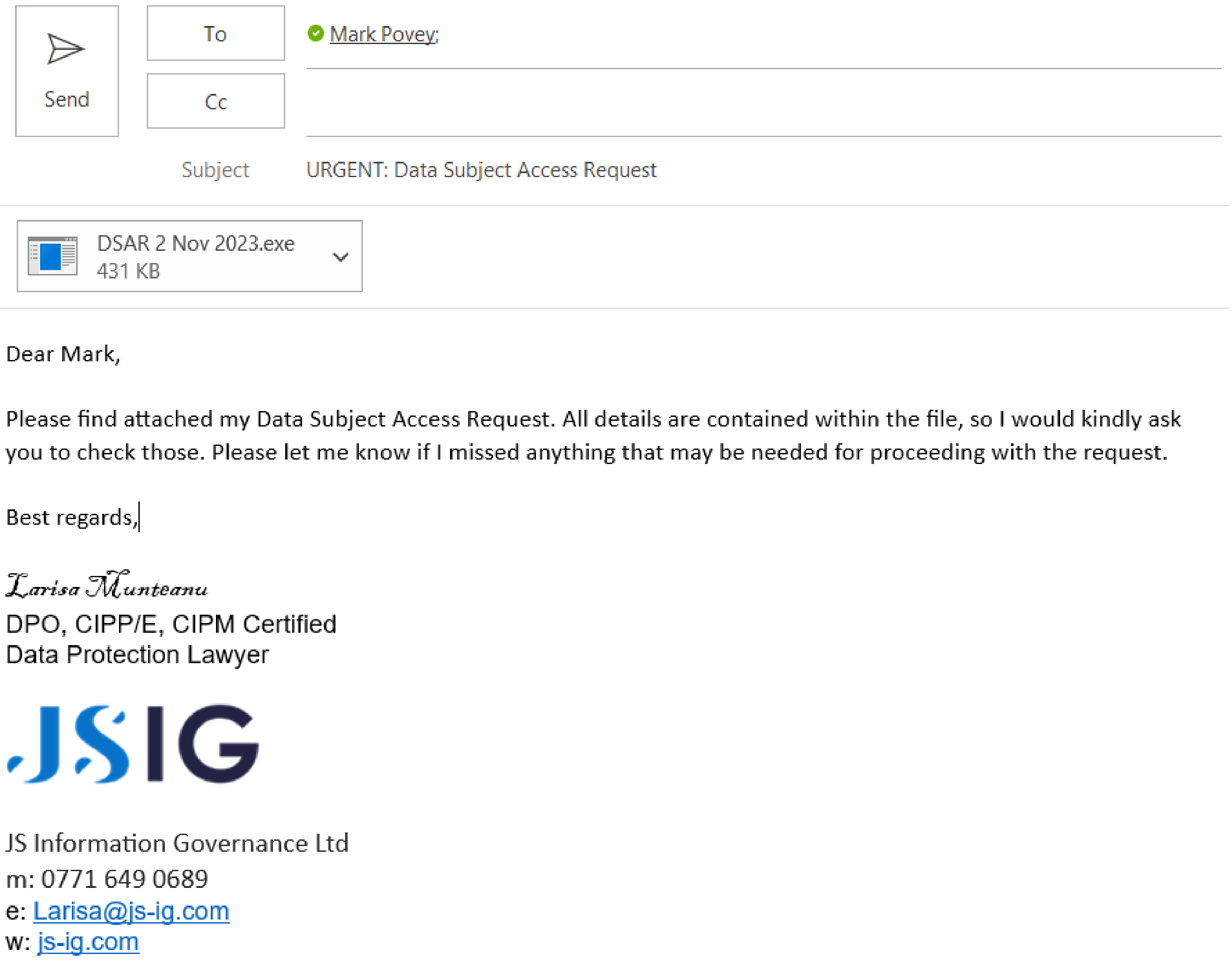
Larisa Munteanu
DPO, CIPP/E, CIPM Certified
Data Protection Lawyer

JSIG

JS Information Governance Ltd
m: 0771 649 0689
e: Larisa@js-ig.com
w: js-ig.com

Malware attack

- The person will try to smoothly insist on you opening the file before the communication chain continues
- As presented before, companies will tend to feel overwhelmed by the context and rush into “proceeding” with the request, out of panic



To: Mark Povey;

Subject: URGENT: Data Subject Access Request

DSAR 2 Nov 2023.exe
431 KB

Dear Mark,

Please find attached my Data Subject Access Request. All details are contained within the file, so I would kindly ask you to check those. Please let me know if I missed anything that may be needed for proceeding with the request.

Best regards,

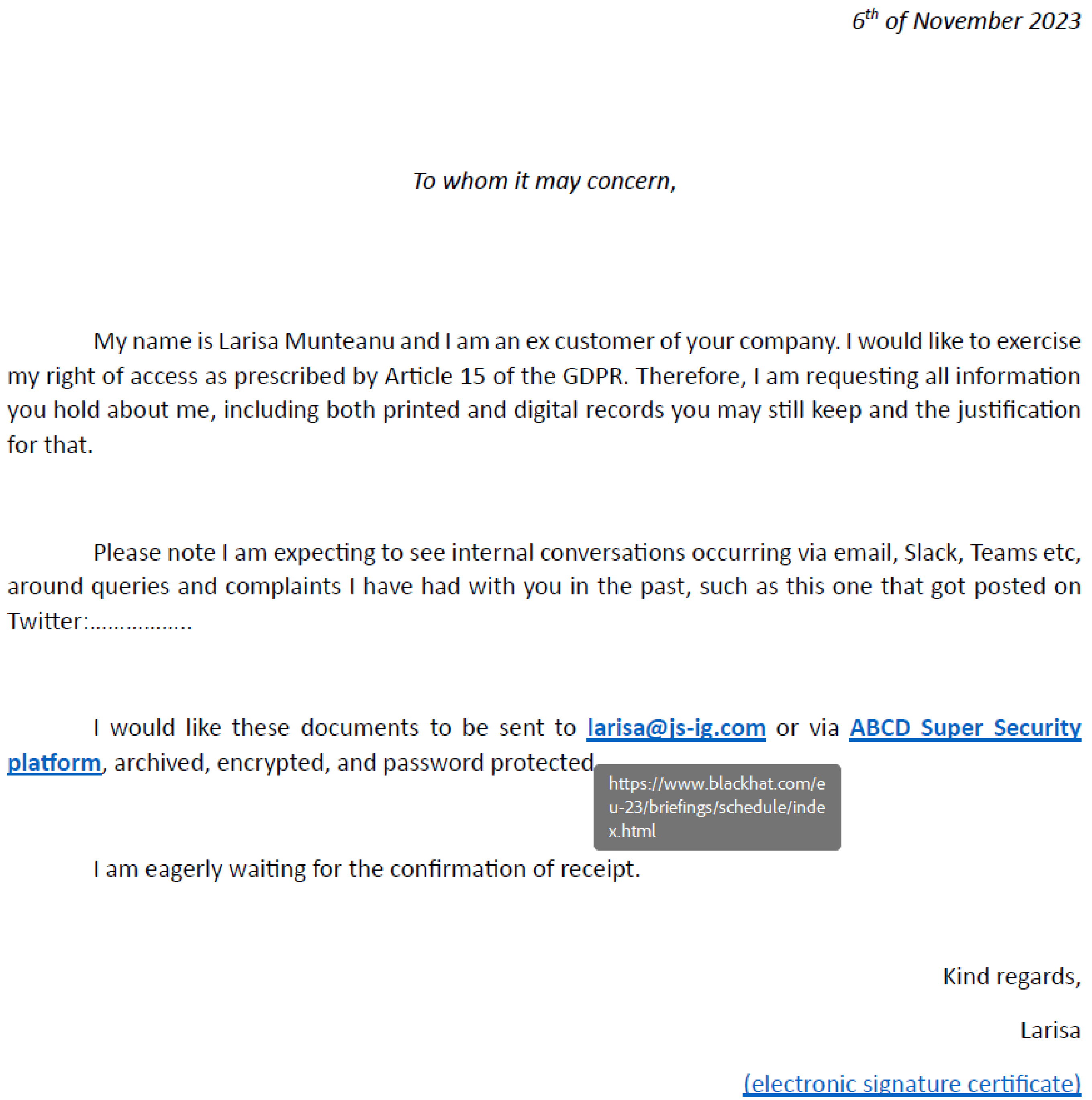
Larisa Munteanu
DPO, CIPP/E, CIPM Certified
Data Protection Lawyer

JSIG

JS Information Governance Ltd
m: 0771 649 0689
e: Larisa@js-ig.com
w: js-ig.com

Malware attack

- Innovation is one of the premises here, so expect the unexpected
- What about pdfs and docs? It can be a hyperlink, multimedia
- Obfuscated text that can be skipped by inspection techniques (it can even be a hidden pdf within the main pdf)



6th of November 2023

To whom it may concern,

My name is Larisa Munteanu and I am an ex customer of your company. I would like to exercise my right of access as prescribed by Article 15 of the GDPR. Therefore, I am requesting all information you hold about me, including both printed and digital records you may still keep and the justification for that.

Please note I am expecting to see internal conversations occurring via email, Slack, Teams etc, around queries and complaints I have had with you in the past, such as this one that got posted on Twitter:................

I would like these documents to be sent to larisa@js-ig.com or via ABCD Super Security platform, archived, encrypted, and password protected.

https://www.blackhat.com/eu-23/briefings/schedule/index.html

I am eagerly waiting for the confirmation of receipt.

Kind regards,

Larisa

(electronic signature certificate)

Vulnerabilities

1. Shared email for privacy matters

- The Data Protection Officer is the privacy guardian of the organisation
- The Data Protection Officer email should belong to… the Data Protection Officer (Privacy Team?)
- How can access controls prevent data breaches via email?
- Is budget a solid constraint for this?

Vulnerabilities

2. Lack of/inadequate training

- Why would training matter?
- How can training be more appealing or dynamic?
- Is budget a solid constraint for this?

Vulnerabilities

3. Policies and procedures that are not supported with corresponding operational measures

- A successful compliance program relies on both theory and practice
- Adequate and appropriate implementation is the key
- How to create a real “human firewall” and protect information assets?
- Is budget a solid constraint for this?

Solutions in 2023

Technology vs Technology

- What types of software should organisations check? (e.g. antivirus, …….)
- What are the main criteria to be used? (e.g. error rate, price?)
- How significant of a problem is it if your budget is extremely limited or you are a start-up?

Rationale vs Impulse

- It is wiser to spend money on security and compliance packages instead of fines.
- Reputational damage cannot be restored with money (and this triggers “leadership” awareness).
- Bigger picture?

Takeaway 1

An apparently valid data protection request is not always legitimate.

Often, they are **used to attack**.

Takeaway 2

Training and company culture are equally important to policies and procedures when it comes to cyber-attacks.

Takeaway 3

Technology can be used against technology.

Q&A