WADIFF CONSULTING

netwrix

The GDPR: Q&A Session

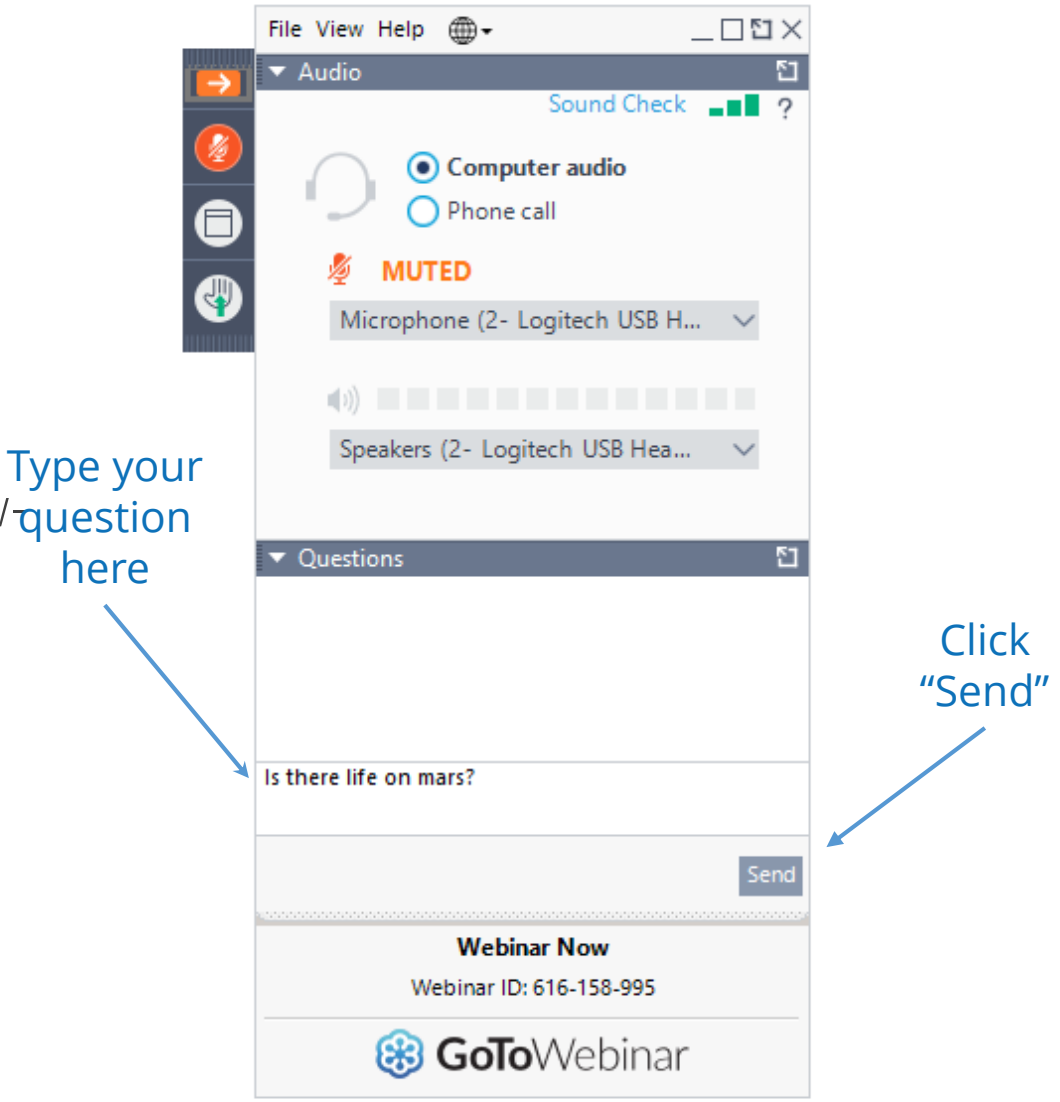
Ian Grey
Information and Cyber Security consultant
ian.grey@wadiff-consulting.co.uk
https://www.linkedin.com/in/iangreyuk

Russell McDermott
Sales Engineer
Russell.Mcdermott@netwrix.com
+44 (0) 203 588 3023 x 2208

Housekeeping

- All attendees are on mute
- Ask your questions!
- Questions will be answered during the session
- You will receive a webinar recording in the follow-up email
- Duration: Up to 60 minutes

We hope you enjoy!



WADIFF CONSULTING

netwrix

If you currently adhere to the DPA what do you need to do differently to comply to GDPR?

If you are a SME in the UK and *fully* comply with the DPA the key changes are:

- Wider definition of personal data – biometrics, genetic etc.
- Rights of individuals are strengthened (e.g. the right to object) and new rights (e.g. data portability)…and need to contact organisations where data has been shared in some circumstances (e.g. rectification and erasure)
- Consent requirements
- Transparency
- 72 hour data breach notification if there are risks to individuals
- Increased obligations for Data Controllers – Accountability, record keeping, privacy by design and by default
- Direct compliance obligations for processors
- Appointing a Data Protection Officer (if you meet the criteria for having one)
- Higher level of fines

WADIFF CONSULTING

netwrix

Our customers details we use are actually their work details (rather than personal details) which are in the public domain (law enforcement officers), is this data subject to the same GDPR policies?

Are photos considered personal data?
I'm thinking about my running club and the team and race photos.

WADIFF CONSULTING

netwrix

"Article 30 record" requirements – if you have less than 250 employees

WADIFF CONSULTING

netwrix

Article 30

If you have 250 or more employees, you must document all your processing activities.

If you have less than 250 employees, you only need to document processing activities that:

- are not occasional; or
- could result in a risk to the rights and freedoms of individuals; or
- involve the processing of special categories of data or criminal conviction and offence data

“The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request. Employees”

WADIFF CONSULTING

netwrix

As a manufacturing company we hold data on our customers – businesses & individuals. We also have a webshop. We also store health information because of the environment we work in about our employees. What do we need to do in order to comply?

Is it possible for relatively smaller business with budgetary constraints, to implement the compliance steps internally without external/third party support?

This all seems very onerous for SMEs like mine - I cannot support a Data Officer and/or will struggle to meet what seems like a massive amount of data systems. Are the guidelines on a "sliding scale" depending on business size?

WADIFF CONSULTING

netwrix

GDPR vs Marketing PECR (Privacy and Electronic Communications regulations)

WADIFF CONSULTING

netwrix

- The UK Information Commissioner's Office website has a lot of guidance a free helpline
- Start with https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr-resources/

The basic steps (there are more, e.g. for Accountability):

- What personal data have I got https://wadiff-consulting.co.uk/2018/04/12/how-to-track-down-your-personal-data-data-mapping/
- Why have I got it (lawful basis for processing + produce Records of Processing Activities https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/
- Should I still have it (retention period - unless there is a legal time period to keep it, you can decide what it is)
- Is it protected (Physical & IT security + training https://ico.org.uk/for-organisations/resources-and-support/posters-stickers-and-e-learning/)
- Can I respond to a Subject Access Request https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/
- Am I transparent in how I deal with the data (Privacy Notice - see https://ico.org.uk/global/privacy-notice/ for an example)

WADIFF CONSULTING

netwrix

When setting up the new privacy statement documents, do we have to get them checked by a legal person or company?

WADIFF CONSULTING

netwrix

Data flows. We are required to show evidence of data flows between systems and to external parties. What methods have you seen used to achieve this requirement?

WADIFF CONSULTING

netwrix

How absolute or not is the data subject right to data deletion/erasure. I'm looking at a system where the underlying data is rendered deleted by breaking the applications links to the data in the DB. The system involves social care so there would be an argument that reviving the data for legal investigation purposes might apply.

WADIFF CONSULTING

netwrix

Right to be forgotten. Personal data can be located in network folders, application databases, the cloud, backups, email, paper files, etc. Let's say a request from an individual to be forgotten is permissible, then finding and deleting their details from all of these locations is a major challenge - particularly for large companies. What challenges are you seeing amongst large companies in complying with the right to be forgotten and what are your recommendations to locate and delete the data?

WADIFF CONSULTING

netwrix

Data retention and deletion. Data for multiple individuals at the end of a retention period is likely to require deletion of that data from multiple locations, including network folders, application databases, the cloud, backups, email, etc. However, you may also find that the data that needs deleting could have different retention periods to other personal data, even in the same database table, as well as across the same database! How then is it possible to comply if we have to keep data X for one reason, but delete data Y for another within the same database? This is a particular challenge in large systems (e.g. HR, Finance, etc.). Yes, we can demand that the vendor perform the deletions required - but even then they would face the same challenges. What approach do you recommend to achieve compliance when the purpose for which data has been retained is at an end, but not so for data that is closely aligned with it?

WADIFF CONSULTING

netwrix

In regards to bought in data, if the supplier states they have consent, how does this work with liability, should we be asking for evidence of their consent?

WADIFF CONSULTING

netwrix

If I share data with sub-contractors can they be bound by my policy?

WADIFF CONSULTING

netwrix

What long term backup media are subject to subject access requests?

WADIFF CONSULTING

netwrix

Who, when, and how will I be audited to see if I am not in compliance?

WADIFF CONSULTING

netwrix

We are hearing rumours that the Privacy Shield may get challenged by the GDPR Working party and fail. Given the ICANN and GDPR argument, what do you think we should do about services we use using US servers?

WADIFF CONSULTING

netwrix

Any ideas about how to convince very small businesses and charities that GDPR is important and applies to them?

WADIFF CONSULTING

netwrix

Is using the Netwrix Tools like shown also in reach for and meant for usage on smaller companies? Looking at pricing / licensing?

https://www.netwrix.com/how_to_buy.html

WADIFF CONSULTING

netwrix

Is the data discovery and classification available via the update option within the current version?

WADIFF CONSULTING

netwrix

Additional module into the same server and DB or does it require extra server/resources?

WADIFF CONSULTING

netwrix

How we can download a trial version of this tool?

https://www.netwrix.com/auditor.html

https://www.netwrix.com/data_discovery_and_classification.html

Next Steps

Contact Sales to obtain more information netwrix.com/contactsales

Data Classification: What It Is, Why You Should Care and How to Perform It
https://blog.netwrix.com/2018/03/15/data-classification-explained-what-it-is-why-you-should-care-and-how-to-perform-it/

What is GDPR: 10 FAQs
https://try.netwrix.com/what-is-gdpr-ebook-nemea.html

GDPR Requirements and Netwrix Auditor Mapping
https://try.netwrix.com/gdpr-compliance-nemea.html

Thank You!

Ian Grey
Information and Cyber Security consultant
ian.grey@wadiff-consulting.co.uk
https://www.linkedin.com/in/iangreyuk

Russell McDermott
Sales Engineer
Russell.Mcdermott@netwrix.com
+44 (0) 203 588 3023 x 2208