GDPR

Compliancy

Part 4 of our series on GDPR and its impact on the recruitment industry

Who are we?

- Dillistone Group Plc, a public company listed on the AIM market of the London stock exchange
- Includes the brands Voyager Software, ISV Software, FCP Internet, Dillistone Systems and GatedTalent

FileFinder Anywhere

isv.online testing and training people

Voyager RECRUITMENT SOFTWARE YOUR BEST CONNECTION

evolve

GATEDTALENT

- Thousands of clients in over 70 countries, both Recruitment and Corporate with some of the largest clients in those fields
- ISO/IEC 17024 GDPR-P certified

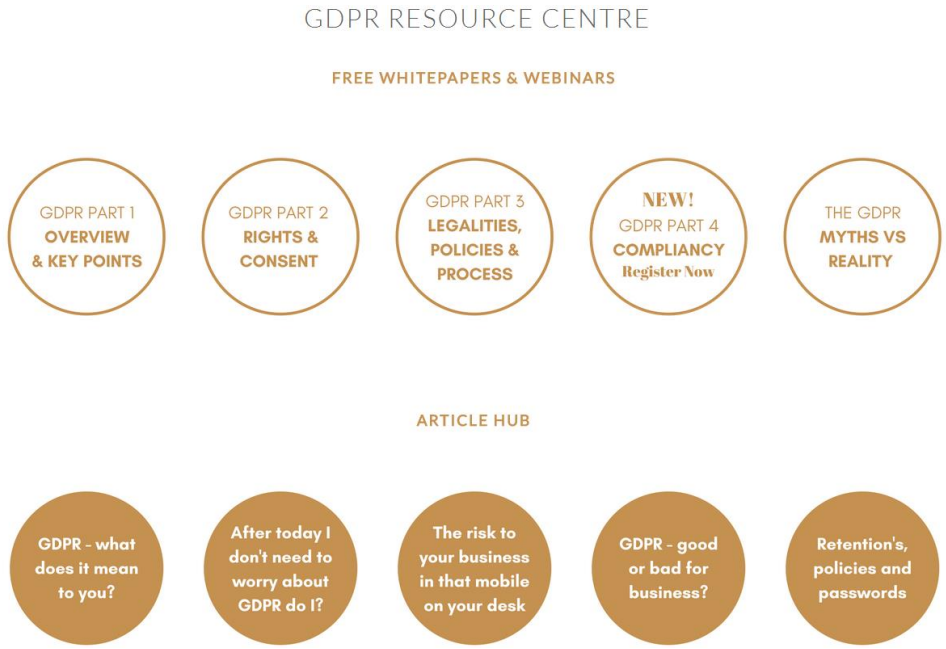
A quick recap

- **Slides & a recording of today's webinar will be available within a few days.**

- In Part 1 of our series we looked at the GDPR in general.
- In Part 2 we looked at consent, rights of data subjects, privacy by design, focusing on Data Protection Officers and data privacy impact assessments.
- In Part 3 we looked at what makes processing legal, controller and processor liability, policies and processes, data security, enforcement and penalties, and certifications.

Catch Up

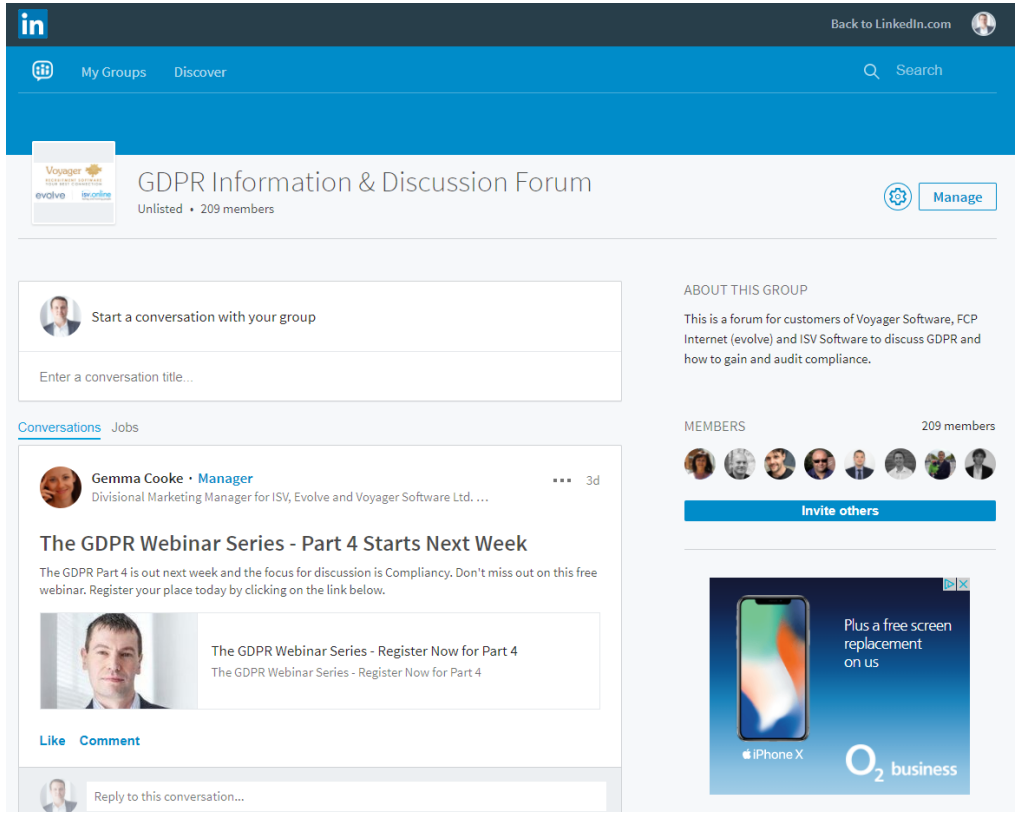
- Recordings of the previous 3 webinars are available online (free of charge).
- Lots of free information available. To find out more, go to…
  - Our GDPR Hub



https://www.voyagersoftware.com/gdpr/gdpr-hub.html

Catch Up

- Or…
  - Our LinkedIn Group



https://www.linkedin.com/groups/8599770

Future Event – GDPR Forum

- Due to the levels of interest we're seeing, we're looking to put on a free in-person event in January

8.15 – 8.45am	Introduction to the GDPR (optional introduction for those less familiar with the GDPR)
8.45am – 9.15am	Welcome refreshments with tea, coffee, pastries
9.15am – 9.30am	Opening Welcome The GDPR and what we're doing about it.
9.30am – 10.15am	Guest Speaking Slot – Speaker TBC
10.15am – 10.30am	Refreshments
10.30am – 12.00pm	GDPR Panel – Q&A Discussion
12.00pm – 12.30pm	General Discussion / Networking
12.30pm	Close

DISCLAIMER

- This webinar is provided for information purposes and is **NOT** intended to be legal advice pertaining to the subject matter
- If you have specific questions on how this may affect your organisation you should consult a legal professional
- Guidance and member state regulator interpretation is ongoing – GDPR is dealing with a highly complex scenario and one size does not fit all
- This is the fourth part of a series of webinars and is therefore not designed to cover everything in one sitting!

This webinar is provided for information purposes and is NOT intended to be legal advice pertaining to the subject matter. If you have specific questions on how this may affect your organisation you should consult a legal professional.

Today

We'll look at:

- With a ticking clock what needs to be done?
- Privacy by Design
- Adopting the GDPR means a culture shift
- Unlawful data- how do you identify it and what can you do about it
- Don't fall into the "compliancy trap"
- Update on what we are doing to help you

ICO- 12 steps to take now

- 1. Awareness – decision makers and key people
- 2. Information – document what you hold
- 3. Communicating privacy information – review and amend privacy notices/Transparency
- 4. Individuals' rights – ensure you can deliver against data subject rights
- 5. Subject access requests – update procedures
- 6. Lawful basis for processing – identify and document. Make it clear to the subject

ICO- 12 steps to take now

- 7. Consent – review how you obtain and record consent – look at historic too
- 8. Children – review consent processes for minors
- 9. Data breaches – ensure you have processes for detecting and reporting
- 10. Date Protection by design and DPIAs
- 11. DPOs – appoint one if you need one, make someone responsible if you don't.
- 12. International transfers – ensure you have an appropriate legal basis

- https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf

How?

- Step 1 – Awareness
  - Right from the top! This has to be a board level issue. They should be briefed on both the risks and the rewards.
  - The board need to support a GDPR compliance project, it will require varying amounts of resources (people money and time) and a “walk the walk” from top management. Have a project plan – there’s more to do than you think.
  - Make a director accountable for the project.
  - Put data protection risk into your risk register – review it regularly.
  - Create a project team (led by someone who isn’t the DPO!).
  - Communicate to and educate your staff.

How?

- Step 2 – Information
  - Do the data mapping exercise we spoke about in the last webinar.
  - Challenge yourself and the stakeholders as you'll likely uncover more.
  - Identify high risk databases (CRM, HR etc).
  - Identify high risk data flows (outsourced payroll).
  - Identify the data categories you process.
  - Look at where you touch the outside world (email, website, devices etc) are they protected?
  - Cull (or gain lawful basis for) data which is not currently compliant.
  - https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf
  - Can you encrypt?
  - Retention policy.

  - DOCUMENT EVERYTHING

How?

- Step 3 – Communication
  - Ensure appropriate privacy notices are in place. You sooner you do this the sooner the data you collect now will be compliant.
  - https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/
  - Make sure you have all your transparency information ready to be given to the subjects.
  - Talk to your suppliers and check their compliance progress.
  - Identify and prioritise necessary contract reviews (employees, clients, candidates & suppliers).

How?

- Step 4 – Individuals rights
  - Using the mapping exercise and/or DPIA check that your procedures cover all the 8 rights.
  - Assess how your systems could help you (eg if you had a deletion request how could you do this?).

How?

- Step 5 –Subject Access Requests
  - Check your policy and process for handling them.
  - Test them.
  - How will you get the data together?

How?

- Step 6 –Lawful Basis
  - Invest time now looking at the types of processing you do and identifying the most appropriate basis for each processing activity.
  - Make sure this is documented. Again, the DPIA/data inventory/mapping exercises will help with this.
  - Review these at suitable periods.

How?

- Step 7 – Consent
  - If you are using it make sure you have clear polices and refresh any existing consents if they are not GDPR complaint.
  - Be careful as an employer.
  - Remember, Consent might arguably be the “safest” but its not the only option open to you.

How?

- Step 8 – Children
  - Unlikely to impact recruitment process, but you might have data that fall under this if you have employee schemes such as childcare vouchers, private healthcare that covers family members etc., employers paying for schooling as a benefit (!)

How?

- Step 9 – Data Breach
  - Make sure you know what a breach is. Denial of access also counts, for example.
  - Put in place incident response and breach reporting process.
  - Make sure you can identify when you might need to inform bodies. SA, subjects, processors or controllers.
  - Test this process.

How?

- Step 10 – Data protection by design and default
  - Know when you are required to do a DPIA.
  - Be able to prove that this is at the forefront of your decision making process.
  - Cyber security staff awareness.
  - Are there any already implemented standards, frameworks or management systems that could contribute (ISO 27001, PCI DSS etc).
  - Should you be externally tested?

How?

- Step 11 – DPO
  - Do you need one?
  - Even if you are not required by law, consider making someone responsible (should you call this role a DPO?).
  - Check for conflicts of interest.
  - “It is most important that someone in your organisation, or an external data protection advisor, takes proper responsibility for your data protection compliance and has the knowledge, support and authority to carry out their role effectively.”

How?

- Step 12 – International Transfer
  - Do you operate in more than one EU member state?
  - If so, you need to designate a lead supervisory authority.
  - Do you have model clauses/BCR where appropriate?

Privacy by Design (PbD)
What does it really mean?

- 7 foundational principles.
- Embeds privacy into information technology, business practices and networked infrastructures.

"With increasingly savvy and interconnected users, an organization's approach to privacy may offer precisely the competitive advantage needed to succeed. Privacy is essential to creating an environment that fosters trusting, long-term relationships with existing customers, while attracting opportunity and facilitating the development of new ones. In an ever-changing world of emerging technologies, the right to privacy is more important than ever. We must remain vigilant in the protection of privacy, the bedrock of our freedom and liberty."

Information and Privacy Commissioner of Ontario

Privacy by Design (PbD)

- 1. Proactive not Reactive; Preventative not Remedial
  - The Privacy by Design approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. Privacy by Design does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

Privacy by Design (PbD)

- 2. Privacy as the Default Setting
  - We can all be certain of one thing — the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.

Privacy by Design (PbD)

- 3. Privacy Embedded into Design
  - Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

Privacy by Design (PbD)

- 4. Full Functionality — Positive-Sum, not Zero-Sum
  - Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum win-win manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security – demonstrating that it is possible to have both

Privacy by Design (PbD)

- 5. End-to-End Security – Full Lifecycle Protection
  - Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved – strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.

Privacy by Design (PbD)

- 6. Visibility and Transparency – Keep it Open
  - Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

Privacy by Design (PbD)

- 7. Respect for User Privacy — Keep it User-Centric
  - Above all, Privacy by Design requires architects and operators to protect the interests of the individual by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

Adopting the GDPR means a cultural shift

- To borrow from the RSPCA: The GDPR is for life not just for Christmas (or 25th May 18 for that matter).
- All the things we have spoken about have to be lived and breathed by an organisation if they want to do the best they can to be compliant and reduce the likelihood of an infringement.
- So how can you do this around your day to day activities?

Adopting the GDPR means a cultural shift

- The key element is awareness. Do staff understand what the GDPR is?
- That in itself is secondary to do they believe, and buy into, why protecting the data and being responsible for it is vital.
- If they can see the importance and the risks, there is a higher likelihood of increased awareness in and around the business.
- Furthermore they are likely to be much more receptive and attentive to any relevant training that you provide.
- You need to plan your education program. Your staff all have their day jobs and you have a business to run. Make sure that you are in a position to follow up and follow through on the training though.
- Must come from top down.

Adopting the GDPR means a cultural shift

- Don’t forget, this is a continuous process so involve staff which all helps the buy in.
- Remember to ensure that new starts into the business are trained to the same level.
- Ask questions of relevant suppliers – The GDPR should be part of any tender process.
- Regularly test your processes.

Unlawful data – how do I find it?

- To find it you have to know what it is.
- That means you need to have defined the criteria which means knowing:
  - 1. Your retention policy
  - 2. Lawful basis you can/will use
    - Consent?
    - Legitimate Interest?
    - Contractual?
    - Legal Basis?
    - Other?
  - 3. Was the data collected lawfully (both under the DPA and the GDPR) in the first place?

Unlawful data – how do I find it?

- Fortunately, the data mapping documents and DPIA that we handed out last time can really help you identify this.
- You should then be a position to know what data you hold that could be considered to be unlawful, so now you have to decide what to do about it!

Unlawful data – what are your options?

- Do nothing (not advised!!!)
- Purge all non lawful existing data
  - Suppliers can help you with this.
- Try and make existing data lawful
  - Remember this needs to be under the GDPR rules.
  - Likely that you will need to send privacy and transparency information.
  - This could be self cleaning.
  - There are tools out/coming that can help with this too.
- Do a bit of both.

- Above all be realistic and pragmatic! Whilst agencies still cling to the notion that the size of their database is a measure of their success. I'd disagree. A much better measure is the volume of active relationships that you have.

The compliancy trap?

“Using XXXXX makes you GDPR compliant”

“Our consultancy service guarantees your GDPR compliance”

“We’ll certify your business to be GDPR complaint”

“Our product is the only one on the market currently that makes you compliant with GDPR”

All these are from real products and services – all these are bovine poo.

There are a lot of myths and legends around the GDPR and this is one of the most popular

(see https://www.voyagersoftware.com/free-whitepapers/the-gdpr-myths-vs-reality.html for more)

The compliancy trap?

The GDPR covers all personal data that you are responsible for, your CRM, your staff, your suppliers and your contacts for example:

Some suppliers will be adapting products and services to help you with your compliance journey, but no-one can guarantee it and these elements will only be successful if used properly. - Which means embedding them into your processes and taking appropriate action if its not followed.

Some suppliers can potentially share responsibility, acting as processors whereby they have an obligation to protect the data accordingly.

What else are we doing to help you?

Within our group we have various streams that we're working on:

1. Education – things like these webinars, the LinkedIn group and our GDPR Hub, along with things like the data mapping templates - aimed at anyone and everyone but with a focus on recruitment.
2. Testing and training – we're producing training and testing packages which you can use internally. Feel free to take one of our GDPR awareness tests! https://goo.gl/ko9f4n
3. Forums and workshops.
4. Data analysis – packages to help you identify potentially at risk data with remedial options.
5. Core product changes – eg privacy audit, SAR, suppression lists, RTBF, privacy/transparency notices and more besides.
6. Privacy management portal – Online privacy management putting the subject fully in control of their relationships.

Next Time…

Article 29 guidance on Breach notification

- Article 29 guidance on Automated decision making.
- Contract changes and data collection notices.
- Offshore data transfers.
- Training your staff.

Reminder

- In addition to this webinar series, there is a LinkedIn group set up which will cover various articles on GDPR, the ePrivacy Directive, checklists to help get you prepared, along with blogs and other features.
- We'll also be using this forum to keep you informed and get your feedback on some of the tools and solutions we're creating to help with some of the challenges of GDPR and potentially help keep you ahead of the competition.
- https://www.linkedin.com/groups/8599770
- Also see the GDPR hub https://www.voyagersoftware.com/gdpr/gdpr-hub.html

Q & A

- Any questions we are unable to get through we'll post the answers on the LinkedIn forum.

- https://www.linkedin.com/groups/8599770