

		<b>ROLE DESCRIPTION</b> <b>GDPR Officer – Commercial Group</b>	
Document: <b>RD.Central</b> <b>Support.GDPR</b>	Issuer: <b>M Clarke</b>	Responsible: <b>AL Fitzgerald</b>	Revision Date: <b>2022-03-31</b>

**Mission statement**

To ensure that the Commercial Group processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.

The following narrative describes the essence of the requirements for the function. However, this does not exclude the incumbent title holder from undertaking accompanying duties that may be required to permit or foster the successful operation of the business.

Serving as the primary contact to the C&I Businesses and under the supervision of the Legal Department, the GDPR Coordinator will primarily be expected to fulfill the below missions:

**1. What:** To document and understand which systems and software are used for storing data and to ensure their use follow the Snap-on cyber security principles.

**Why:** To minimize the risk of a breach and assist in the event of a reported security incident.

**How:** By undertaking the following:

- Ensure all systems/software are vetted for conformity through consultation with IT and onboarded pursuant to company policies.
- Set-up an approval process for any new system/software purchase to be vetted for conformity before purchase and provide contracts to Data Protection Manager for inclusion of data protection requirements.
- Ensure all stakeholders understand cyber security risks and how to avoid them
- Act as a coordinator for collecting information in the event of a security or data incident, as directed by the Legal Department.

**2. What:** To ensure all the relevant stakeholders are familiar with what GDPR means in their role and what constitutes personal data and support the implementation of the principles of Privacy by Design.

**Why:** To ensure the Commercial Group is always compliant when obtaining, storing and

*Any hard copy of this document is uncontrolled and potentially obsolete. Consult the SNA Europe Intranet for the latest revision.*

processing personal data

**How:** By undertaking the following:

- Targeted training and refresher sessions (targeted by topic and by audience)
- Conducting “on the spot” internal/internal audits, and address *potential issues proactively*
- Creating audit trails (e.g. who changed what and when)
- Ensuring local understanding of the protocol for reporting suspected security or data incidents.
- Participating in regular Privacy by Design training as provided by the Data Protection Manager and deploying those principles within the Business Units.

**3. What:** Ensure each Business Unit has a clear retention policy or policies (depending on the country requirements)

**Why:** To ensure all the stakeholders are aware of how long they can retain the data

**How:** By undertaking the following:


- Working with the appropriate legal responsible to ensure the retention policy/policies are in place
- Review those policies with the relevant stakeholders on a yearly basis
- Include checks on this issue in the internal/internal audits

**4. What:** Central point of contact for the completion of requests of data subjects

**Why:** Data subjects have the right to access any personal data held about them. A request to access personal data is known as a Data Subject Access Request (DSAR). The time limit for a response to a DSAR starts from the day the request is received (whether it is a working day or not) until the corresponding calendar date in the next month.

**How:** Interfacing with the Data Protection Manager to support communications with data subjects. Assist in the local process to ensure that the DSAR is being completed in line with the GDPR’s requirements e.g.

- Check the identity of the person making the request
- Remove any information about someone else (third-party information) from the material
- A well-designed and up to date information management system to locate and extract data and redact third party data

	<b>ROLE DESCRIPTION</b> <b>[Job title]</b>		
Document: <b>RD.Central</b> <b>Support.GDPR</b>	Issuer: <b>M Clarke</b>	Responsible: <b>AL Fitzgerald</b>	Revision Date: <b>2022-03-31</b>

**5. What:** Ensure each Business Unit is completing and maintaining the required documentation for compliance with the Company's data protection framework.

**Why:** To ensure that there is a control environment in place for the maintenance of required documents and information.

**How:** By undertaking the following:

- Work with the Business Unit to complete and maintain data mapping and privacy notices.
- Ensure contracts that require data protection agreements are reviewed and kept in accordance with retention policies.
- Assist in the completion of Data Protection Impact Assessments as required.
- Work with Business Unit to identify new websites, mobile apps., marketing campaigns and customer documents to ensure accurate notices and cookie consents are presented.
- Coordinate data privacy/GDPR audits performed by Snap-on Internal Audit; support the audited Business Unit in preparing the management response to Internal Audit reports; implement the findings of Internal Audit Reports at the audited Business Unit level and expand such findings across C&I other Business Units for harmonization purposes.

### Measurements of Success:

The role will be measured on the following criteria with targets set including:

- Maintenance of current data maps.
- Maintenance of up to date and current privacy policies.
- Timely completion of data subject rights requests.
- Regularly scheduled training with Business Units.
- Timely reporting of security or data incidents.
- Completeness of data protection agreements in relevant contracts.
- Timely participation in training events and reviews with the Data Protection Manager.

### Knowledge, Skills and Abilities

- Strong knowledge of EU data privacy (including in the context of Brexit) and data protection regulation, and a good understanding of other major privacy frameworks and evolving legislation worldwide.
- Sufficient knowledge of information technology and data management systems required.

*Any hard copy of this document is uncontrolled and potentially obsolete. Consult the SNA Europe Intranet for the latest revision.*

- Well-developed and professional interpersonal skills; ability to interact effectively with people at all organizational levels of the firm and in a multicultural environment.
- Ability to work independently, exercise leadership, and influence change.
- Excellent writing and presentation skills.
- A legal background and recent experience in compliance/audit would be a plus

Revision History		
Date	Issue	Notes
YYYY-MM-	[Description]	

*Any hard copy of this document is uncontrolled and potentially obsolete. Consult the SNA Europe Intranet for the latest revision.*