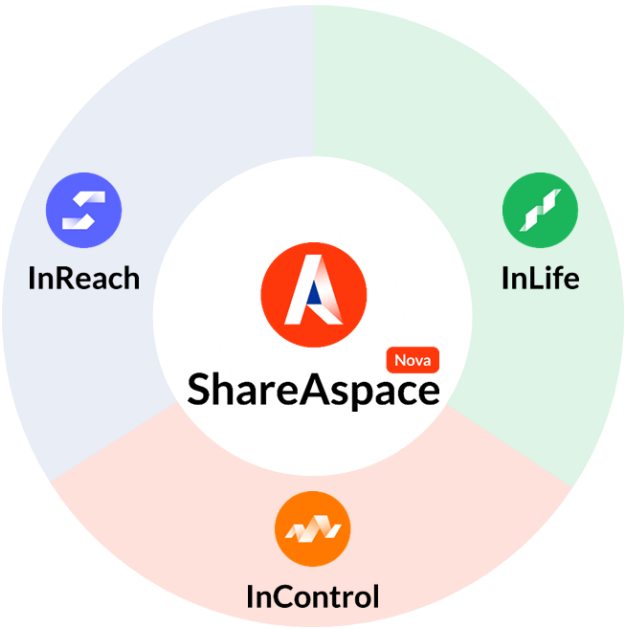
Eurostep...for secure, through-life, product-centric collaboration



Export Control, ITAR and ShareAspace

Author	**Eurostep**
ID/Version:	ESSM-6-962

Eurostep
info@eurostep.com
www.eurostep.com

Export Control, ITAR and ShareAspace

1. Why do countries have Export Control Regulations

Many countries have regulations designed to protect their capabilities, both in commerce and defence. Generally these are known as Export Control Regulations. They are designed to stop both physical objects and related data, including software and design data, falling into "the wrong hands", thereby protecting that country's interests.

Perhaps the best known such regulations are the International Trade in Arms Regulations coming from the United States. Known as ITAR, these are designed to protect the USA's lead in defence and carry big penalties for infringement. However these are not the only US regulations and the USA is not the only source for such regulations. ITAR applies to anything coming from the US that has military applications. This can even include material that was created outside of the US.

It is important to be aware that some items that, at first sight are for civilian use, can be subject to Export Control because they are used in the design or manufacture of defence products. Thus, for example, the design data set for a civil aircraft may contain such items.

Export Control Regulations include the management of physical items. Here we focus on the data around such items, referred to as ECR data. The regulations can apply when ECR data is simply shown on a screen to the wrong person or in the wrong place. This demonstrates that conformance to the regulations relies on people behaviours as well as what can be done with IT systems. Physical access also has to be controlled to IT systems that hold ECR data.

2. What does this mean for data sharing

If data is covered by Export Control Regulations, there will typically be a licence that defines who can see that data. Thus additional controls have to be put in place for that data. Only those entitled to see the data will be granted access. Limitations will also be applied to ensure that the data can only be extracted or copied in conformance with the relevant licence. It is also typical to track who has accessed the ECR data.

Fortunately the core functions needed to satisfy these requirements are essentially similar to those used to protect Intellectual Property and not all data is subject to export control. However it is typical for large systems to contain a number of ECR controlled parts. The additional constraints must then be applied to those items in particular as an additional layer of protection. Access control (and tracking) is needed at the level of individuals as well as organisations. Once this is in place, data access and sharing processes are the same.

3. ShareAspace and ECR controlled data

ShareAspace has been designed to enable and facilitate controlled sharing of data. It already has many of the controls needed for handling ECR data. These can be used in line with ECR regulations by aligning ShareAspace's user roles and organisations to ECR licences. This approach provides an ECR control solution suitable for use within organizations that have matching overall processes in place for ECR data. A software product, such as ShareAspace, can only ever be an enabler for achieving ECR conformance and must be accompanied by suitable processes and training for personnel, including partner organizations.

Eurostep is planning to further enhance ShareAspace as a tool for handling ECR data in 2018. ShareAspace is the ideal software when the need is to share a mix of ECR data and non-ECR data involving potentially many ECR licences.