



Stabilisation Unit

FAQs on Duty of Care

Duty of Care Approach

Stabilisation Unit
April 2017

1. GENERIC QUESTIONS

What is duty of care (DoC)?

Employers have a duty of care to their employees, which means that they should take all steps which are reasonably possible to ensure their health, safety and wellbeing.

In the UK, duty of care legislation is predominantly based on Common Law and therefore arises from precedence with little written legislation. This means that the law around duty of care is often a 'grey area'.

However, what is indisputable is that the employer always owns the duty of care for an employee, whilst undertaking their duties.

Duty of care is also based on 'love thy neighbour' (an obligation of one party to take reasonable care for another in all the relevant circumstances). A contractual relationship isn't needed to instil DoC obligations.

For inherently dangerous work a greater degree of care must be taken (Hopps v Mott MacDonald Ltd [2009]).

What can lead to DoC responsibilities?

The leading judicial test for a duty of care in England was found in the judgments of Caparo Industries plc v Dickman, in which the House of Lords set out the following three-part test:

- a) Harm to the other party is foreseeable;
- b) The parties are in a sufficiently close relationship (proximity);
- c) It is fair, just and reasonable that a duty of care should be recognised.

DoC can also arise where:

- d) One party reasonably relies on the other acting for his or her protection;
- e) One party exercises control over the circumstances giving rise to the danger (e.g. signing off the security posture in country as fit for purpose)
- f) One party assumes responsibility for the circumstances giving rise to a danger (e.g providing PPE etc);
- g) Specialist advice is given.

Who is responsible for my/a deployee's Duty of Care?

In UK legislation, duty of care always rests with the employer (whoever pays the wage) when undertaking paid activity; this can't be delegated, abrogated, divested or transferred. However, the risks and risk management to uphold DoC can be shared and DoC obligations apply based on the 'proximity' of a party to the activity/individual.

From an SU perspective this means that legal DoC is usually held by:

- Crown Agents for DCEs deployed on a CA contract;
- PUS (of the relevant department) for those deployed on an HMG contract;
- The relevant Chief Constable for a deployed police officer.

How is DoC fulfilled?

As it would be unreasonable to expect the DoC holder to manage and mitigate all the risks inherent in a deployment, especially the in-country safety and security, the risk of the deployment is shared between a number of partners. These are likely to be:

- Whoever holds DoC (as the ultimate responsible stakeholder);
- The Stabilisation Unit as the deploying body and delegated SRO for DoC for deploying police officers and those on HMG contracts;
- The policy holding department as the stakeholder responsible for the activity taking place;
- The in-country platform (Embassy, DfID country office or multilateral mission) as the safety and security guarantor overseas.

Why does the SU act as the SRO for HMG or police deployments?

Firstly it is worth pointing out that the SU is the only part of government which deploys international police officers and those on HMG contracts to multilateral missions in Fragile and Conflict Affected States (FCAS).

In recognition of this, HMG's Network Board (the cross-Government board of departmental Chief Operating Officers responsible for overseeing international deployments of HMG personnel) has delegated the responsibility for managing and ensuring DoC for those deployed through the SU to our Director (Mark Bryson-Richardson) as the SRO.

How does the SU fulfil this role?

The day-to-day management and assurance of DoC for those deployed by the SU is the responsibility of the Head of Deployments. This is fulfilled by assuring the compliance of the relevant mitigation measures in which are the responsibility of the various stakeholders and overseeing the SU's preparation of deployees.

The SU manages and mitigates its Duty of Care risk by:

- Training the deployees in the skills necessary for the specific platform and country they are deploying too;
- Ensuring the physical and psychological wellbeing of our deployees is administered;
- Providing our deployees with professional in-house security advice;
- Acting as a guarantor of platform security and treating, tolerating, transferring or terminating the risk where necessary;
- Ensuring their generic welfare is considered in-country (accommodation, food, r&r etc);
- Being a focal point for deployees issues or concerns whilst on, and subsequent to, deployment.

Why does the SU take such a strong line in ensuring DoC?

Whilst delays or difficulties with a deployment in most areas can be tolerated, and little significant impact felt, failures in DoC can lead to direct harm or worse. Therefore, the SU takes its obligations to those who are deploying through us to assist HMG's agenda overseas very seriously. This can mean that our DoC requirement can significantly delay or even stop activity where we feel the risks are too high and mitigations are not sufficient.

2. WHAT DOES THIS MEAN FOR ME?

For an HMG task holder:

As the deployee is going under a contract from my HMG department, am I responsible for DoC?

No, whilst the DoC does sit in law with your PUS, the management of this has been assigned to the SU. To avoid complications and unclear DoC authority, any issue relating to DoC must be passed to the SU to manage.

What are my obligations to ensure DoC?

You are to ensure, at the earliest opportunity, that the platform you are deploying the selected individual to is aware that this activity will be happening, will be responsible for their in-country safety and security and that the deployee will come under the platform's safety and security procedure. This should be articulated to the platform's security section as well as the mission's senior responsible owner (HoM, DHM, SRSG etc).

You are to ensure that your pre-deployment briefing for the deployee fully covers all the issues related to their welfare, discipline and safety and security. For example, if you require the deployee to be covered by the Armed Forces Act, it is your responsibility to make this clear and ensure the deployee and SU are aware.

For a Deployee:

The DoC provisions I'm being expected to abide by are overly onerous, can I 'opt-out' of these?

No, it is not possible to pick and choose which elements of SU/HMG DoC you wish to abide by. HMG has a legal obligation towards all deployees and its judgements, restrictions and regulations are in place with this in mind. Nor is it possible to sign yourself out of HMG's DoC. If HMG/SU has deployed you, and is paying you, they are responsible for your DoC and no agreement or notification can change that.

We do accept that restrictions imposed by HMG can sometimes be more stringent than restrictions you have been placed under by other private employers. However, this is down to an interpretation of UK Common Law and HMG's desire to demonstrate 'best practice'.

The platform/multilateral organisation I have been deployed to say they hold my DoC and I should not engage on this issue with SU/HMG, is this correct?

In UK Common Law this is not correct, unless you are receiving your salary directly from that institution (e.g. you receive a UN/EU/OSCE etc pay statement) and it is the bulk of your earnings for the activity you are undertaking (this does not include hazardous allowances).

In the UK system your employer (whoever pays your salary) holds your DoC and this cannot be transferred. In SU terms this will usually be Crown Agents, the FCO or your Chief Constable (for police deployments).

What in-country platforms will be asked to take on is your in-country safety and security provision in line with that which their own employees are covered. This is not the same as full DoC and enables the SU to

step-in on your behalf if we feel the safety and security system you are in is failing or the obligations and assurances around your safety and security we have been given are not being met.

We recognise that this interpretation does not always align with that of some institutions, but it is in line with UK Common Law, and for the SU/HMG, this is what prevails.

For an in-country platform:

I have been asked to take on the safety and security of a deployee, does this mean I'm responsible for their DoC?

No, you will not be taking on legal DoC as this will always reside with their employer. By taking on the in-country safety and security you are facilitating the delivery of DoC on behalf of the employer who, without a toehold in the country, has limited knowledge of the location or ability to manage the deployees exposure to risk.

By accepting the in-country safety and security, the expectation is that the deployee will be treated in the same manner as all of your employees at that location or all visitors from your head office or home department.

This means that they must be included in any evacuation or contingency plan (if in place); their logistics and movements must be conducted in accordance with the platform protocols, as must any close protection or wider security requirements and they must receive the same security briefing and support as required for any other employee or visitor.

The SU does not expect the in-country safety and security provider to go above or beyond what they would do for any other employee visiting that location.

I don't feel I can guarantee the safety and security of a deployee to the same standard as my own staff – for example they will be staying at a hotel and not in embassy accommodation, can I refuse this support?

Whilst the SU will seek to be flexible where possible and will highlight that your safety and security provision should be reasonable and practical (for example we will be aware that you do not own or have authority over an independent hotel, as would a UK court), our ability to deploy an individual is based on in-country safety and security being assured.

If you feel you cannot support the deployment you need to inform the SU at the earliest opportunity. Obviously this may put any subsequent deployment at risk.