Turning a DPIA into an integrated business process

13th Annual Nordic GDPR summit 25 May 2020
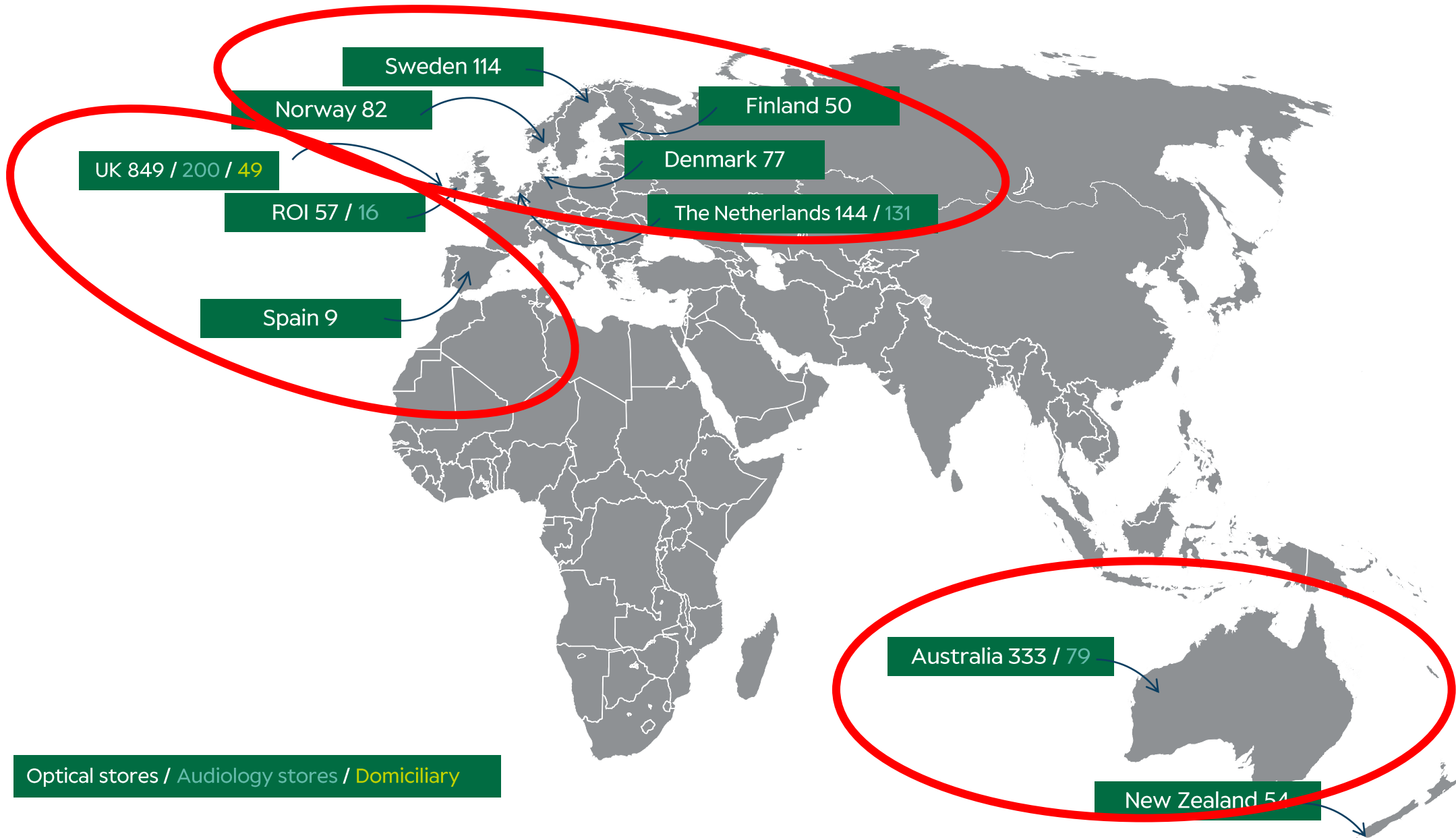
10 markets – 3 regions - more than 2,000 stores

Sweden 114

Norway 82

Finland 50

UK 849 / 200 / 49

Denmark 77

ROI 57 / 16

The Netherlands 144 / 131

Spain 9

Australia 333 / 79

New Zealand 54

Optical stores / Audiology stores / Domiciliary

Our market share per country

Customer volume – September 2019

Nr 1.	Nr 3. (Joint third)	Nr 3.	Nr 1.*	Nr 1.	Nr 1.
43	19	17	28	32	36
Denmark (glasses)	Finland (glasses)	Netherlands (glasses)	Netherlands (audiology)	Norway (glasses)	Sweden (glasses)
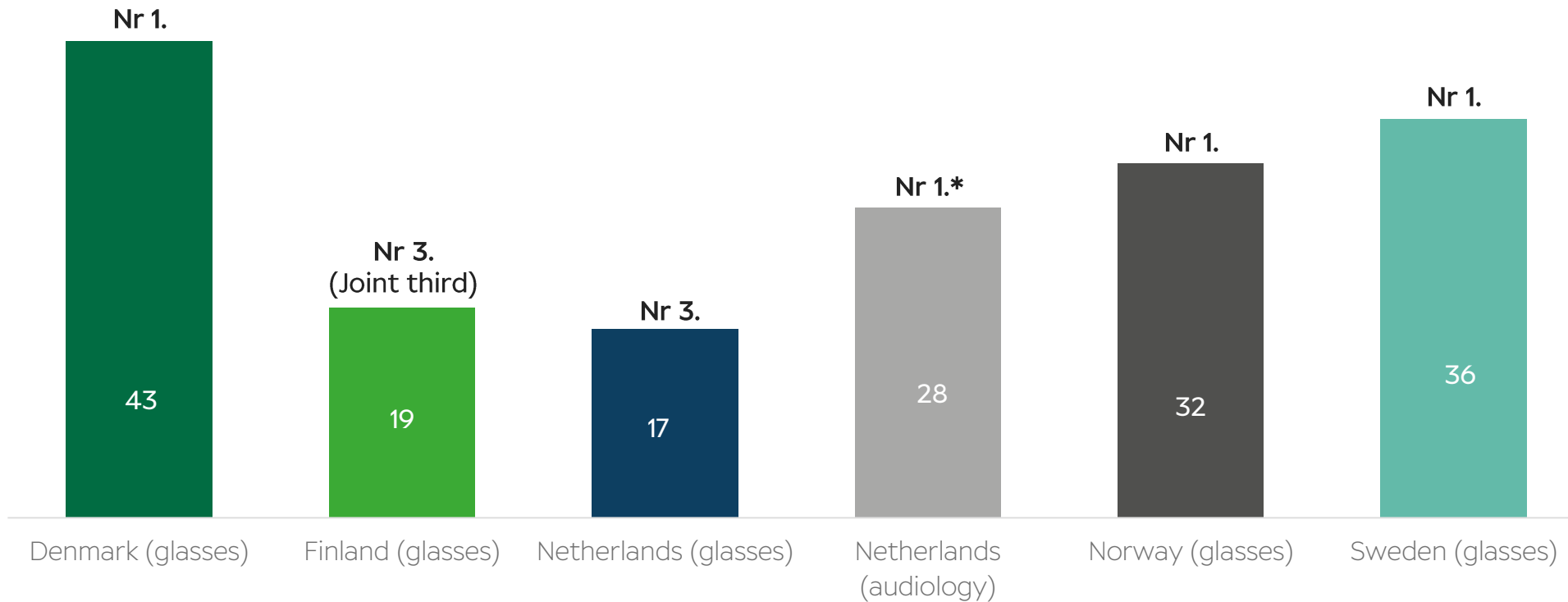
Data Protection is essential for Specsavers as the:

"Licence To Operate"

The year 2018/19 in numbers

£2.78 billion
group revenue

6%
increase on 2018/19 revenue

400,000
group revenue

530 million+
contact lenses sold

21.6 million+
frames sold

3,000+
partners

37,000+
employees

2,111
optical stores and audiology centres

1.6 million+
customer feedback responses

816,000+
followers on Facebook

1.4 million+
visitors to our website every day

The way we work

The everyday behaviours that support our strategy, purpose and values

Focus on the Customers

we always consider and act in the best interests of our customers

Support the partnership

we work with our partners to understand our business, develop our brand and grow

Act as one team

We work for one international company and support each other to reach our goals

Make it happen

We plan and execute brilliantly, and review and improve as we go

4 focus areas within Data Protection

IT Tech

Privacy by design

....

by making it easy for users

Legal

Ensuring GDPR principles

....

and other legal obligations

Compliance

Prove what you do

....

by documenting & making controls

Culture

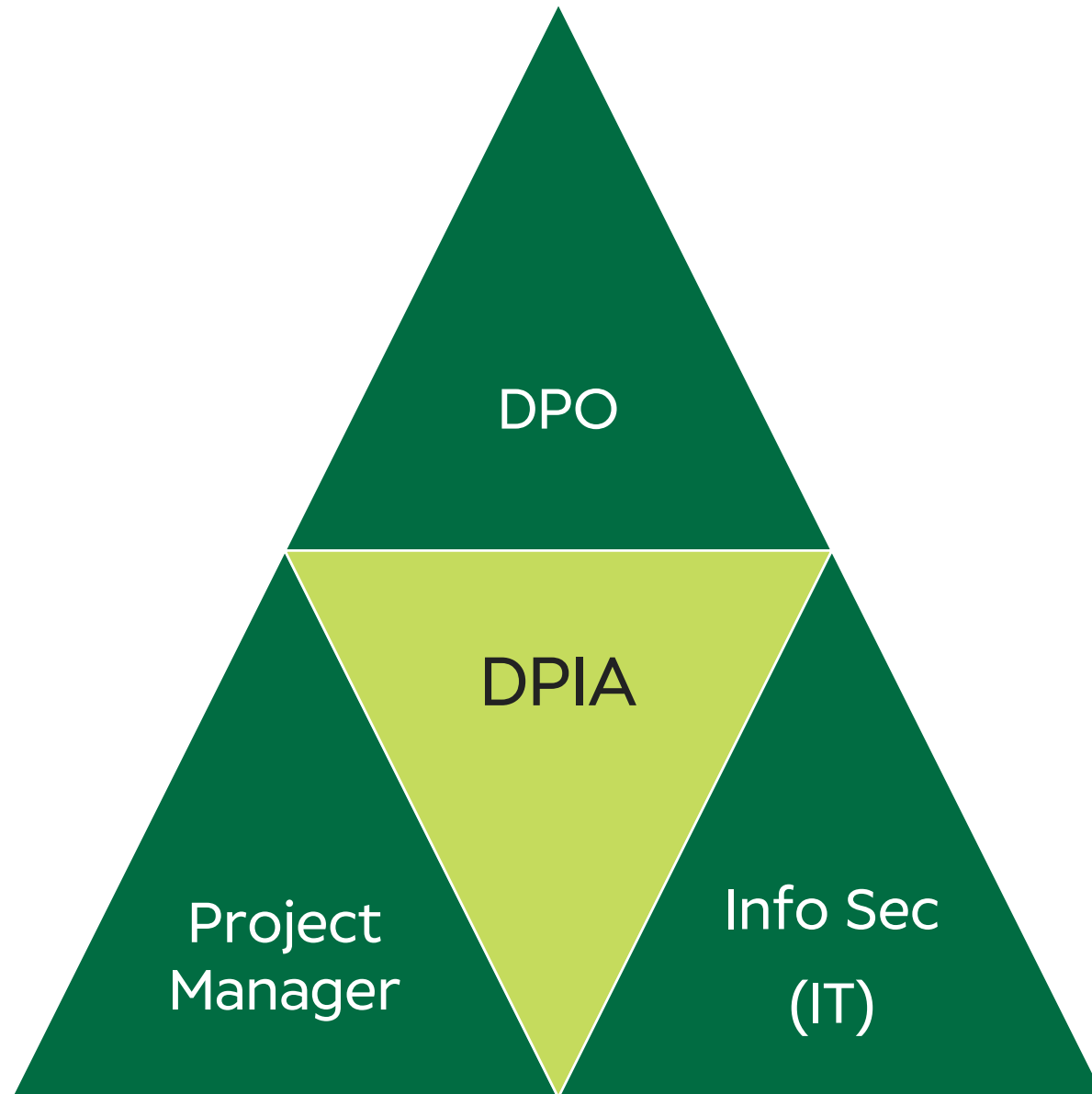*Protect PII data*

....

as if it was your own
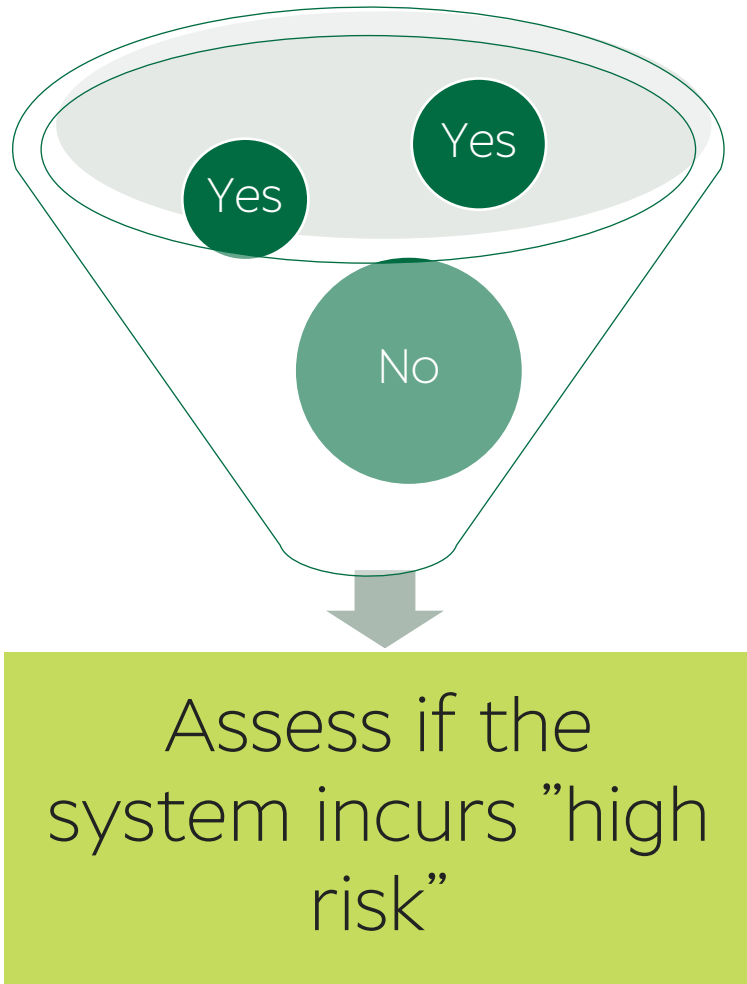
DPIAs in Specsavers

- **Stakeholders:** Specsavers have more than 200 commercial and technical project managers

- **Frequency:** Since 2018 we have assessed more than 100 projects involving PII

- **Nature:** Projects can be either new processes or (more often) driven by new software.

A triage process

Initial stage of DPIA: Assess the level of risk by using a funnel model

- ✓ Does the system proces PII?
- ✓ Data regarding *vulnerable persons?*
- ✓ *Sensitive data (art 9)?*
- ✓ *Extensive volume?*
- ✓ *Surveillance/Monitoring purpose?*
- ✓ *Extended Geographical Scope?*
- ✓ *Extended processing purpose?*

Yes

Yes

No

Assess if the system incurs "high risk"

Second stage of DPIA: Describe & Evaluate

Final Stage of DPIA: Risk assessment

Impact (CIA)

			Little impact on any or all of the following: ->Customers affected - Individual ->Brand image – Little embarrassment ->Financial Loss - Minimal ->Regulatory/Legal issues - No implication ->Operational issues – Minimal	Minimal impact on any or all of the following: ->Customers affected - Few ->Brand image - Potentially embarrassing, Internal to the company ->Financial Loss - Marginal ->Regulatory/Legal issues – Operating challenges	Minor or localised impact on any or all of the following: ->Customers affected - Partial ->Brand image - Potentially embarrassing, Disrepute in the business industry ->Financial Loss - Substantial ->Regulatory/Legal issues - Report to be sent to concerned authorities	Major impact on any or all of the following: ->Customers affected - Many ->Brand image - Disrepute at the national level ->Financial Loss - Large ->Regulatory/Legal issues - Formal investigation by RA, Legal disputes ->Operational issues - Large technical downtime, large scale	Critical impact on any or all of the following: ->Customers affected - Most ->Brand image – Critical brand impact ->Financial Loss – Business threatening ->Regulatory/Legal issues – Fines, legal action ->Operational issues – Prolonged outages
			VERY LOW 1	**LOW 2**	**MEDIUM 3**	**HIGH 4**	**VERY HIGH 5**
Likelihood	>60% - Very likely, The event is expected to occur in most circumstances as there is a history of regular occurrnace.	Very Likely 5	15	30	45	60	75
	<60% - There is a strong possibility the event will occur as there is a history of frequent occurrence	Probable 4	12	24	36	48	60
	<40% - The event might occur at some time as there is a history of casual occurrence	Possible 3	9	18	27	36	45
	<10% - Not expected but there's a slight possibility it may occur at some time	Unlikely 2	6	12	18	24	30
	<1% - Highly unlikely, but it may occur in exceptional circumstances. It could happend, but probably nevery will.	Conceivable 1	3	6	9	12	15

Risk Evaluation Scoring

Risk evaluation is a process that is used to compare risk analysis results with risk criteria in order to determine whether or not a specified level of risk is acceptable or not.

High	>45	High Risk	Risk Acceptance - Senior Management level (SIRO, CIO, SEC)
Medium	18 to 44	Medium Risk	Must be mitigated.
Low	1 to 17	Low Risk	Continues Monitoring.

1. Highlight the risk

2. Analyse it

3. Execute identified actions

4. Conclude if the risk is:

- Mitigated
- Reduced
- Accepted

Thank you for your attention

Any Q´s feel free to contact me

Lene.Refsgaard@Specsavers.com