Perché è importante essere preparati? (1)

- Evitare rischio di sanzioni per:
  - mancata collaborazione (fino ad **Euro 20 milioni** o al **4% del fatturato mondiale** dell'esercizio precedente)
  - dichiarazioni o attestazioni false o notizie o circostanze o produzione di atti o documenti falsi (**reclusione da sei mesi a tre anni**)
  - Interruzione o turbamento intenzionale degli accertamenti (**reclusione sino ad un anno**)

Perché è importante essere preparati? (2)

- **Disturbo** alla normale attività d'impresa e impatto sull'umore dei dipendenti
- Possibile avvio di procedimenti penali sulla base di **indizi di reato** acquisiti durante le ispezioni
- Se la società è **quotata**, il valore delle azioni può scendere repentinamente (perché gli investitori diventano nervosi avendo appreso la notizia)

Perché è importante essere preparati? (3)

- Il primo passo **imprescindibile** per le autorità per verificare e/o integrare informazioni su presunte violazioni:
  - acquisite **d'ufficio**, a seguito di **segnalazioni** o in settori individuali nel **piano ispettivo semestrale**
- Prima **difesa** contro accuse di violazioni:
  - Impugnazione validità accertamento per violazioni procedurali
  - Maggiori possibilità di archiviazione **senza accertamento violazioni**

Perché è importante essere preparati? (4)

- Nuovo principio di «*Accountability*»:
  - **Documentabilità** (anche durante le ispezioni) delle scelte organizzative delle imprese
  - Approccio **meno formalistico** delle autorità, anche durante le ispezioni
  - **Maggiori risorse** (finanziarie e personale) a disposizione delle autorità di controllo
  - Inevitabile aumento di **numero delle ispezioni**

Come prepararsi?

- **Registro** dei trattamenti
- **DPO** se presente (atto di nomina) e **struttura organizzativa** (e.g., privacy *champions*)
- **Procedure** interne (*e.g.*, gestione *data breach*, *data minimization*)
- Risultati **audit periodiche** di adeguamento
- Materiale **formazione** privacy del personale
- Qualunque altro documento idoneo a **provare** le scelte dell'impresa in merito alle **misure organizzative adottate a tutela della privacy**

All’arrivo dell’autorità

- È essenziale, per ragioni di sicurezza:
  - annotare i nominativi dei funzionari
  - fornire il **badge** di riconoscimento (con nome e titolo)
    - **il capo ispezione** rappresenta di solito l’autorità ed è il **punto di contatto** con gli avvocati e l’azienda
  - Informare i dipendenti che è iniziata l’ispezione e che è necessario collaborare ma mantenere la **confidenzialità** e non comunicare all’esterno (neppure familiari) nulla di quello che sta succedendo
  - chiedere ai funzionari se sono in corso altre ispezioni presso altre sedi o abitazioni di dipendenti
    - organizzarsi per fornire assistenza legale

Alcuni aspetti pratici

- Controllare il provvedimento che autorizza ispezione
- Firmare il foglio di entrata
- Assicurarsi che sia disposta una sala dedicata all'ispezione
- Coordinare la comunicazione interna ed esterna

Il Team

- Team interno strutturato e pronto a prestare assistenza legale
- Consulenti esterni specializzati
- DPO, management e altri dipartimenti (specialmente IT e *Media relation*)

Il Team

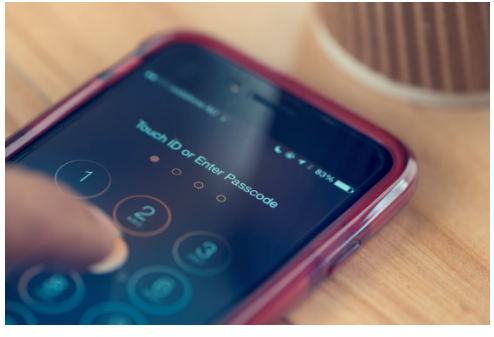
- Ripartizione dei compiti nel team:
  - membri del gruppo **nell'ufficio dei legali esterni**
  - team di avvocati **presso l'azienda**
  - **team leader** che coordina e si occupa di eventuali disaccordi con i funzionari

Poteri dei Funzionari nel corso di un *dawn raid*

- Esaminare e fare copie di documenti (in formato cartaceo ed elettronico)
  - **investigazioni digitali**
- Richieste informazioni al **personale**
- Ispezionare locali, automobili, valigette, armadi (abitazioni ed autovetture private)
- Apporre **sigilli** ad uffici, armadi, registri, ecc.

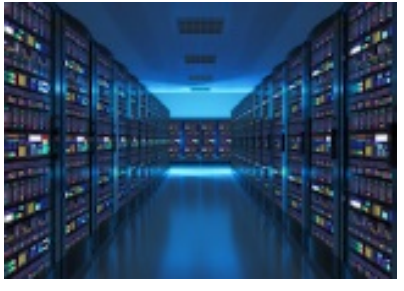
Ispezioni digitali

- Gli ispettori possono ispezionare
  - Dispositivi IT: **server**, computer fissi, portatili, *tablet* e tutti i dispositivi mobili
  - Supporti di memorizzazione: CD, DVD, chiavi USB, hard-disk esterni, nastri di backup, servizi *cloud*...
- Vale anche per dispositivi personali utilizzati per fini aziendali



Il ruolo dell'IT: accesso ai server

- Gli ispettori possono accedere ai server della società
- Se dati di accesso sono detenuti da *admin* non presente in sede (es. *headquarter* o società esterna)
  - includere una sezione dedicata nel protocollo di *best practice* interno
  - autorizzazione per i Server globali
- Non creare nuovi account o modificare/creare password nel corso dell'ispezione



Cosa e come cercano gli agenti

- Gli ispettori possono utilizzare:
  - Strumenti di ricerca per keyword
  - *Forensic IT tools* (strumenti per ricerca e *forensic copy/ imagine*)
- Blocco temporaneo caselle posta elettronica
- Assistenza dell'IT manager aziendale
  - Domande su architettura sistema, chiavi accesso

Prove digitali

- Tutte le informazioni contenute nei file in formato digitale:
  - documenti di testo, corrispondenza, disegni, foto, database...
- Anche se **cancellati** e/o **metadati**:
  - informazioni sui file, *path-name*, dettagli di invio e ricezione...

Ispezione dei dispositivi

- I documenti potenzialmente rilevanti sono
  - Raccolti, indicizzati e revisionati in loco
- Ispettori stabiliscono se documento è rilevante, ma la società può contestare la valutazione
  - *legal privilege* o
  - ambito oggettivo dell'investigazione

Il ruolo dell'IT: cosa può fare per difendere al meglio l'azienda

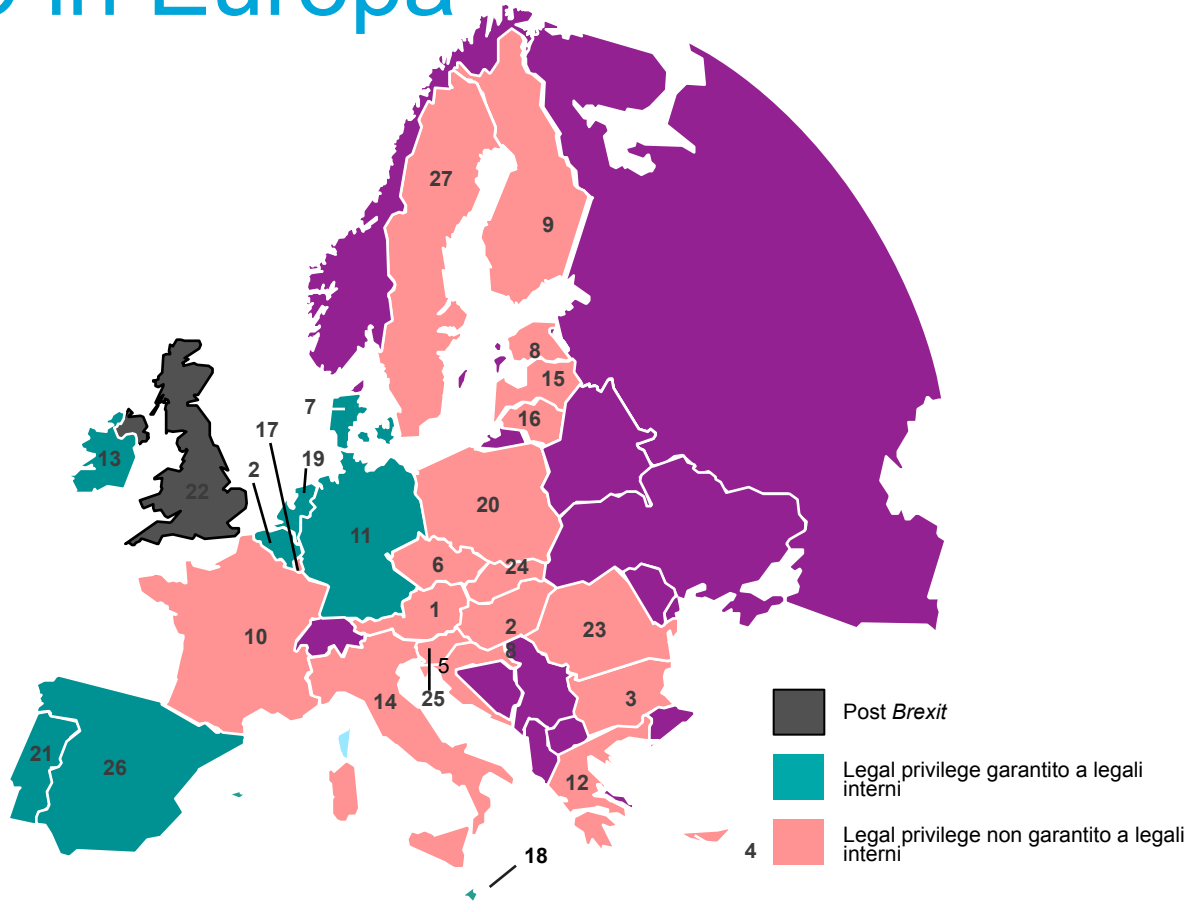
- I funzionari non possono prelevare:
  - File ed email che risalgono ad un periodo non interessato dal contenuto delle indagini
  - File ed email che non riguardano il contenuto delle indagini
- In caso di copia del *hard-disk*:
  - far annotare che l'azienda si oppone (così da poter sollevare la questione in un eventuale giudizio)
  - richiedere che una copia digitale sia messa in una busta sigillata e chiedere un

Legal Privilege

- Esprimere subito il dissenso ai funzionari sulla lettura o copia dei documenti protetti
- Fornire informazioni sul documento per giustificare
  - come ad esempio: l'autore, il suo indirizzo, lo scopo del documento e in che circostanze è stato redatto (senza svelare il contenuto)
- Consentire ai funzionari di dare un breve sguardo al documento solo se non determinante a rivelarne il contenuto
- In caso di discussione, se i funzionari rifiutano di utilizzare la busta sigillata, far registrare la vostra opposizione nella minuta dell'ispezione

Legal Privilege in Europa

1. Austria
2. Belgio *
3. Bulgaria
4. Cipro
5. Croazia
6. Repubblica Ceca
7. Danimarca
8. Estonia
9. Finlandia
10. Francia
11. Germania
12. Grecia
13. Irlanda
14. Italia
15. Lettonia
16. Lituania
17. Lussemburgo
18. Malta
19. Olanda
20. Polonia
21. Portogallo
22. Regno Unito
23. Romania
24. Slovacchia
25. Slovenia
26. Spagna
27. Svezia
28. Ungheria



* I legali interni non sono ammessi all'iscrizione all'ordine belga. Tuttavia, esiste un albo parallelo riservato ai legali interni, istituito per legge, con regole deontologiche, di indipendenza e disciplinari, altrettanto stringenti rispetto a quelle previste per gli iscritti all'ordine degli avvocati

Richieste d’informazioni

- Discutere l’ambito dell’ispezione e identificare i dipendenti chiave cui potrebbero essere rivolte richieste d’informazioni
- Suggerire ai funzionari il dipendente adatto a rispondere alle domande
- E’ possibile farsi assistere da un legale esterno in quanto non ha natura penale
- Rivedere con il legale esterno il verbale prima di sottoscriverlo
- Sollevare obiezioni se necessario e assicurarsi che siano registrate

I Sigilli

- Se i funzionari appongono un sigillo ad un ufficio o ad un archivio, assicuratevi di:
  - fare una foto al sigillo, in modo che se presenta alterazioni al momento in cui viene applicato, l'autorità non può accusarvi di averlo forzato il giorno dopo
  - avvertire tutte le persone interessate – incluso lo staff delle pulizie e la sicurezza
  - mettere una persona a guardia della stanza sigillata tutta la notte
  - se possibile, fare in modo che l'entrata della stanza sigillata sia filmata da telecamere di sicurezza

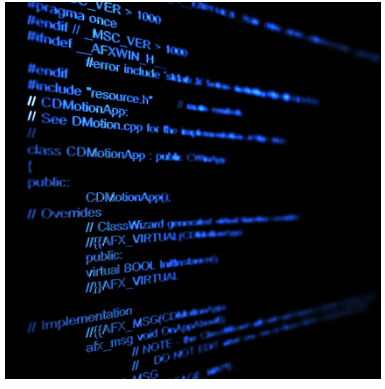
Prima che gli Ispettori vadano via

- Rivedere tutti i documenti copiati, le minute, commenti opposizioni fatte nel corso dell'ispezione
- Ricordarsi che l'azienda non può rifiutarsi di firmare il verbale
- Concordare con gli ispettori la lista di eventuali parti da chiarire / documenti da fornire o aree di conflitto
- Fare un indice ed una copia esatta di tutto quello che viene prelevato

- Chiedere rispetto confidenzialità sui documenti prelevati laddove possibile
- Chiedere una copia delle note prese dagli ispettori comprese domande fatte e risposte ricevute

Al termine dell'ispezione (prove digitali)

- L'azienda riceve lista e copia di tutti i documenti rilevanti all'interno di un CD/DVD
  - viene generato *Hash Value che* identifica il percorso dei singoli file, garanzia di non modificabilità, integrità e tracciabilità (*chain of custody*)
- Agenti devono cancellare dai propri dispositivi ogni traccia dei documenti revisionati
  - «*in maniera tale che i dati non possano essere in alcun modo ricostruiti*»
- Verificare con attenzione che non vengano presi documenti non pertinenti all'oggetto dell'ispezione



Cosa fare dopo l’ispezione

- Informare tutti i dipendenti che l’ispezione è finita ma che bisogna continuare a mantenere la massima confidenzialità sull’accaduto
- Rivedere la documentazione prelevata e le informazioni acquisite, e valutare se ci sono prove incriminanti
- Decidere se impugnare l’ispezione per qualsiasi irregolarità
- Decidere se l’azienda deve bloccare eventuali violazioni in corso che sono state evidenziate

Cosa fare dopo l'ispezione

- Procedere ad un *audit* interna completa (revisione dei documenti ed informazioni fornite verbalmente dai dipendenti) per verificare se ci sono altri elementi utili
- Redigere un rapporto delle sedi visitate, i dipendenti cui sono state rivolte domande, i documenti consegnati, le informazioni prelevate, in modo da ricostruire il quadro della situazione
- Informare la casa madre se ci sono altre sedi coinvolte e quindi a rischio di ispezione
- Considerare se notificare agli *auditor* e/o agli assicuratori qualora appropriato
- In caso di società quotate, considerare se in base alla normativa vigente è necessario fare un comunicato stampa

Domande?