REGIONE DEL VENETO
ULSS2 MARCA TREVIGIANA

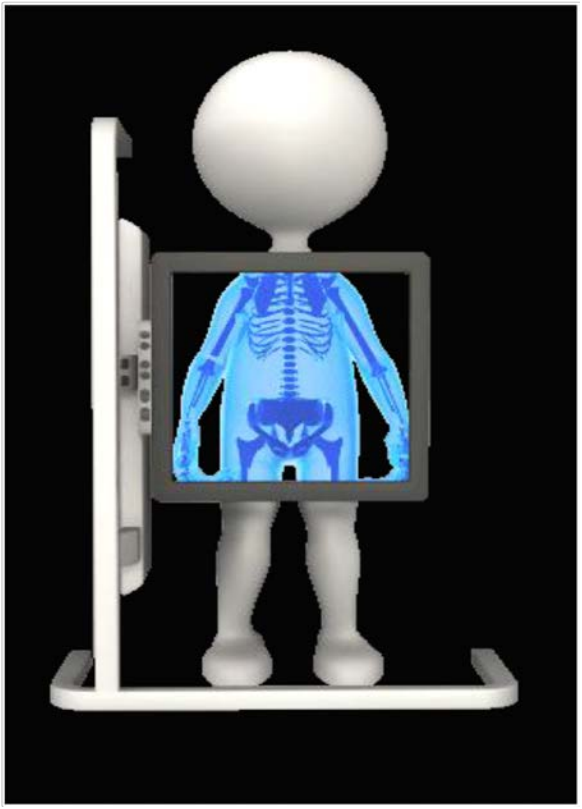
LA NUOVA NORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Treviso 07/03/2018

Ufficio Pivacy
Dr.ssa Cristina Canella

Prendersi cura del paziente oggi…

..significa prendersi cura anche dei suoi dati



In ambito medico l'osservanza delle disposizioni relative al trattamento dei dati sono rilevanti non solo ai fini dell'applicazione della disciplina di settore (Codice privacy), ma anche del rispetto del Codice di deontologia medica.

(art. 11 Riservatezza dei dati personali, 12 Trattamento dei dati sensibili, 25 Documentazione sanitaria, 26 Cartella clinica, 34 Informazione e comunicazione a terzi, 78 Tecnologie informatiche)

LE PRINCIPALI NOVITÀ IN AMBITO NORMATIVO

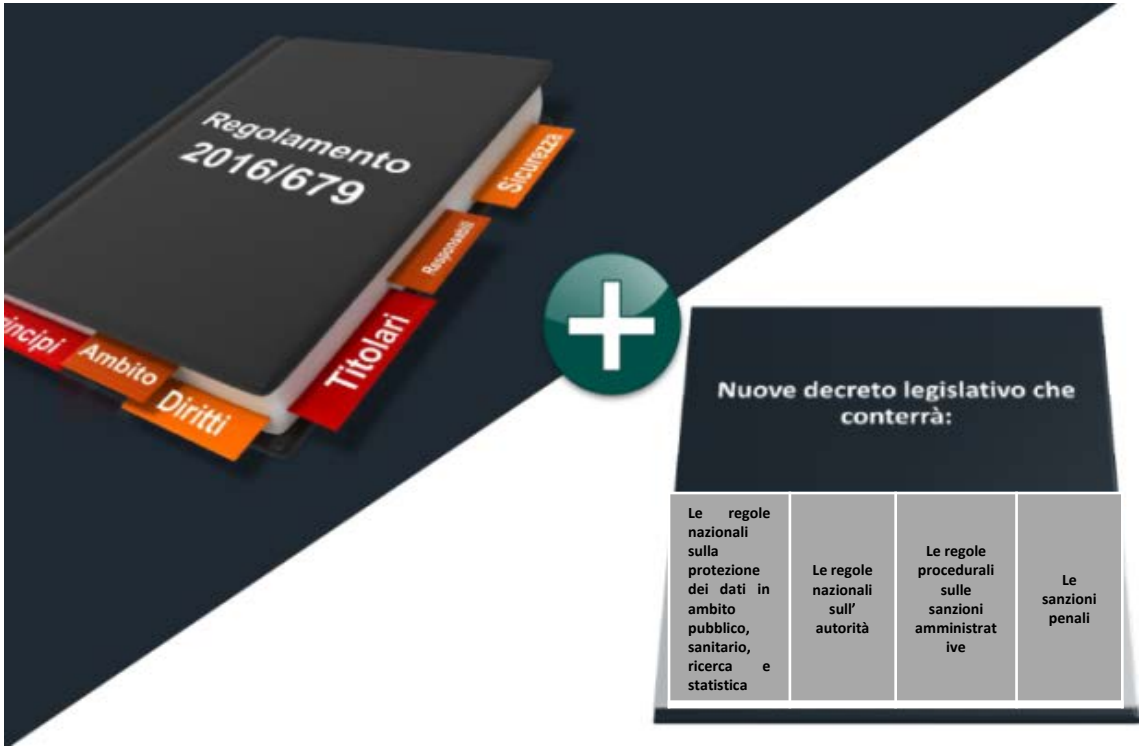
- ✓ Decreto legislativo 30 giugno 2003 n. 196
- ✓ Codice in materia di protezione dei dati personali
- ✓ *Direttiva comunitaria 95/46*
- ✓ *Regolamento Comunitario in materia di data protection*

NEW

REGOLAMENTO EUROPEO (UE) 2016/679

REGIONE DEL VENETO
ULSS2 MARCA TREVIGIANA

1. EVOLUZIONE DELLA NORMATIVA, REGOLAMENTO EUROPEO (UE) 2016/679



Nuove decreto legislativo che conterrà:

Le regole nazionali sulla protezione dei dati in ambito pubblico, sanitario, ricerca e statistica	Le regole nazionali sull' autorità	Le regole procedurali sulle sanzioni amministrative	Le sanzioni penali

173 Considerando - indicano la motivazione degli articoli dell'atto

99 articoli

Il nuovo Regolamento, già approvato, entrerà in vigore il 25 maggio 2018

2. Quali adempimenti per i Titolari del Trattamento a partire dal 25 maggio 2018?

Occorre rifare tutto da capo?

REGIONE DEL VENETO
ULSS2 MARCA TREVIGIANA

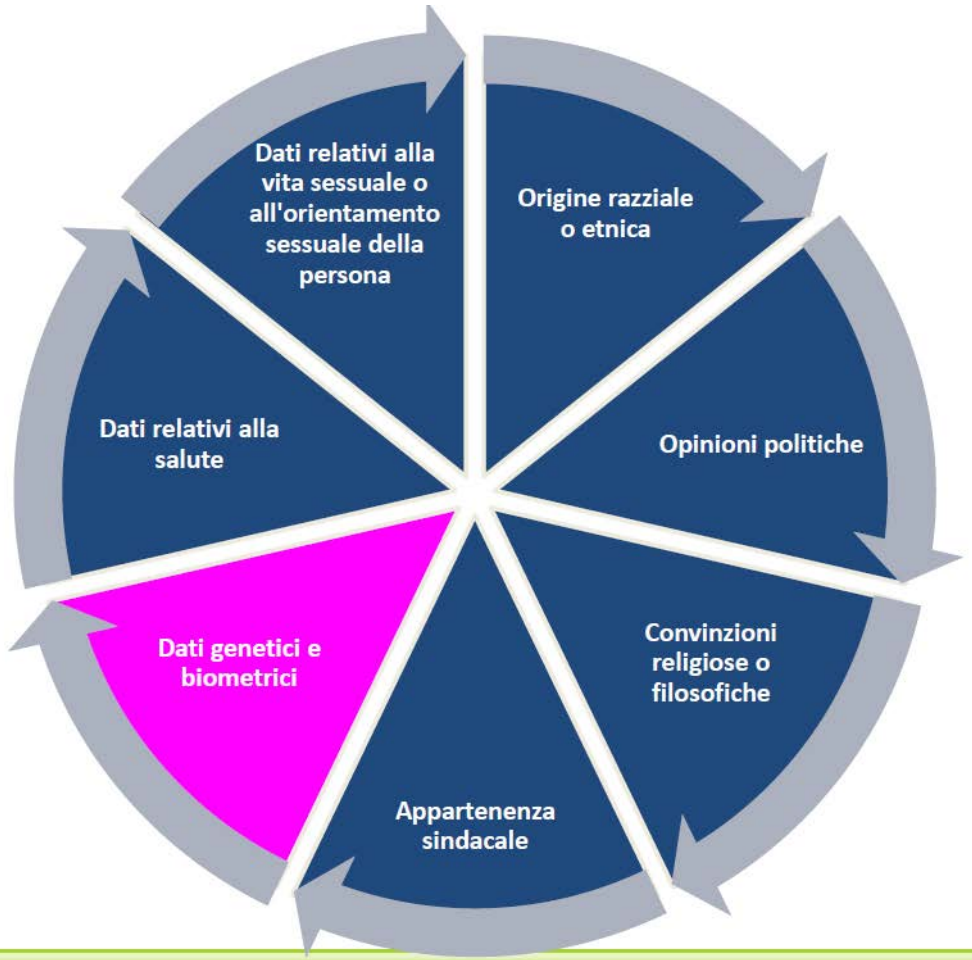
COSA RESTA

1. GLI **OBBLIGHI** E **RESPONSABILITA'** IN CAPO AL TITOLARE DEL TRATTAMENTO
2. LA DEFINIZIONE DI DATO PERSONALE, CON LA SOLA AGGIUNTA DEI DATI GENETICI E BIOMETRICI. I DATI RELATIVI ALLA SALUTE SONO DEFINITI DATI SANITARI
3. LE **RESPONSABILITÀ PER LE VIOLAZIONI PRIVACY** DA CHIUNQUE COMMESSE (VERTICI APICALI E SUBORDINATI)
4. LE VARIE **INFORMATIVE** PRIVACY: UTENTI,DIPENDENTI, SITO WEB, FORNITORI ETC
5. IL **CONSENSO** AL TRATTAMENTO, ANCHE SE SARA' ESPRESSO CON MODALITA' DIVERSE
6. LA NOMINA DEGLI **OUTSOURCER** QUALI **RESPONSABILI** DEL TRATTAMENTO
7. LA PREVISIONE DELLE **MISURE IDONEE** DI SICUREZZA IN MODO PARTICOLARE PER I TRATTAMENTI AUTOMATIZZATI
8. LA PREVISIONE DELLE SANZIONI **PENALI, AMMINISTRATIVE** E **CIVILI**

REGIONE DEL VENETO
ULSS2 MARCA TREVIGIANA

COSA CAMBIA

1. L'OBBLIGO DELLA TENUTA DEL **REGISTRO DEI TRATTAMENTI**
2. MENO BUROCRAZIA, **PIÙ RESPONSABILIZZAZIONE.** MAGGIORE ATTENZIONE ALL'ANALISI DEL PROCESSO DI TRATTAMENTO DEI DATI PERSONALI
3. L'OBBLIGO DI COMUNICARE AL GARANTE PRIVACY LE VIOLAZIONI PRIVACY (DATA BREACH)
4. L'OBBLIGO PER ALCUNI TITOLARI DI NOMINARE UN **DPO/RPD**
5. SCOMPARE LA FIGURA DEL **RESPONSABILE INTERNO** PRIVACY, EVENTUALMENTE DA SOSTITUIRE CON IL «DELEGATO PRIVACY»
6. VIENE MENO L'OBBLIGO, SANZIONATO, DI NOMINARE PER ISCRITTO GLI INCARICATI DEL TRATTAMENTO. TALE FIGURE ASSUMERANNO IL RUOLO DI PERSONE AUTORIZZATE
7. SUPERAMENTO DELLE MISURE MINIME DI SICUREZZA: SI PASSA AL CONCETTO DI ADEGUATE MISURE DI SCUREZZA
8. PER ALCUNI TRATTAMENTI, IL CUI ELENCO DOVRÀ ESSERE FORNITO DAL GARANTE PRIVACY, SCATTERA' L'OBBLIGO DI EFFETTUARE UNA VALUTAZIONE DI IMPATTO PRIVACY
9. MAGGIORE «ATTENZIONE» SUI TEMPI DI CONSERVAZIONE DEI DATI



Resta il doppio regime basato sulla maggiore o minore "sensibilità" del dato

Dati genetici: dati personali relativi alle caratteristiche genetiche ereditarie che forniscono informazioni sulla fisiologia o sulla salute della persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

Dati biometrici: dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono l'identificazione univoca, quale l'immagine facciale.

REGIONE DEL VENETO
ULSS2 MARCA TREVIGIANA

CONSENSO

COSA CAMBIA

- Per i dati sensibili il consenso deve essere esplicito;
- non deve essere necessariamente documentato per iscritto; il titolare deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento;
- per i minori è valido a partire dai 16 anni.

COSA non CAMBIA

- Deve essere libero, specifico e inequivocabile e non è ammesso il consenso tacito o presunto.

GLI ELEMENTI DI NOVITÀ: PRINCIPIO ACCOUNTABILITY

Voce del verbo dimostrare

Il titolare del trattamento è:

↓

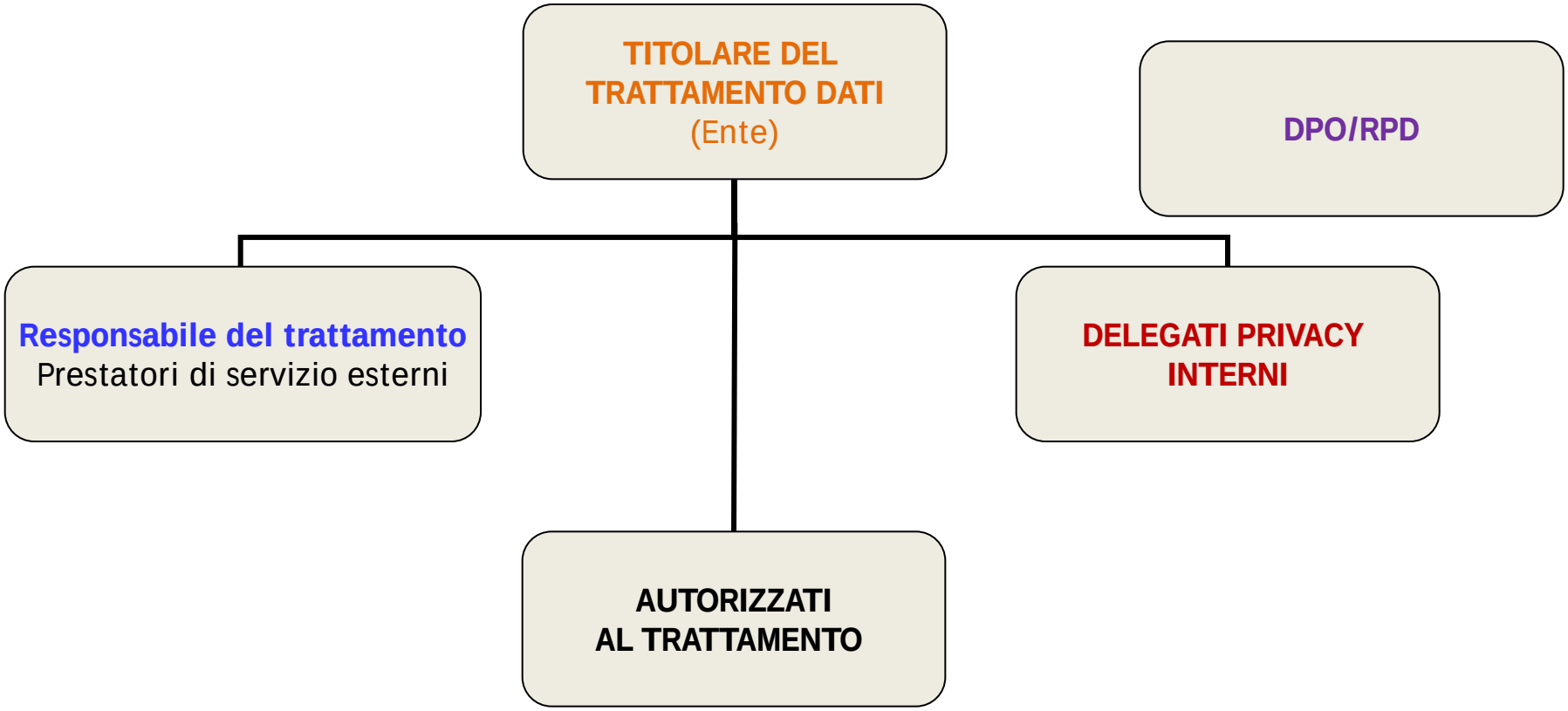
competente per il rispetto dei principi applicabili al trattamento di dati personali

↓

in grado di comprovarlo («responsabilizzazione»)

REGIONE DEL VENETO
ULSS2 MARCA TREVIGIANA

CAMBIA ORGANIGRAMMA PRIVACY



REGIONE DEL VENETO
ULSS2 MARCA TREVIGIANA

SICUREZZA DEL TRATTAMENTO (Art. 32 del GDPR)

Secondo un approccio basato sul rischio, Il Titolare del Trattamento e il Responsabile del Trattamento mettono in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono:

- La pseudonimizzazione e la cifratura dei dati personali
- La capacità di assicurare su base permanente, la riservatezza, l'integrità, dei sistemi e dei servizi di trattamento
- La capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico;
- Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza dei trattamenti

Qualche consiglio pratico per adeguarsi al GDPR

Per prepararsi al GDPR,i titolari del trattamento devono assicurarsi che i trattamenti da loro effettuati siano conformi ai principi privacy previsti dall'articolo 5, paragrafo 1, del Regolamento, tra i quali particolare rilievo assumono quelli della trasparenza e della minimizzazione dei dati.

I titolari del trattamento- sia essi privati che Pubblica Amministrazione- devono rivedere ed aggiornare gli esistenti programmi di Compliance Privacy, in modo particolare aggiornare le **policy inter**ne, modulistica ed i piani di risposta ai Data Breach (obbligo generalizzato). Particolare attenzione dovrà essere riposta nella costruzione del Registro dei trattamenti (obbligo generalizzato) e nei trattamenti che dovessero richiedere il DPIA (Valutazione di Impatto privacy)

Tra i vari fondi e risorse economiche accantonate dai Titolari e destinata alla compliance privacy, una buona parte dovrà essere convogliata alla formazione del DPO e del personale interno.

Tali programmi di formazione dovranno essere strutturati in modo da offrire una conoscenza generale e complessiva del GDPR, ma soprattutto dovranno "*calare*" la privacy nel settore in cui opera il Titolare.

LE REGOLE PER L'AUTORIZZATO AL TRATTAMENTO

REGOLE PER L'AUTORIZZATO AL TRATTAMENTO

Trattamento dati *con* l'ausilio di strumenti elettronici e/o informatici

Trattamento dati *senza* l'ausilio di strumenti elettronici e/o informatici

REGIONE DEL VENETO
ULSS2 MARCA TREVIGIANA

REGOLE PER L'AUTORIZZATO AL TRATTAMENTO
TRATTAMENTO CON STRUMENTI INFORMATICI

- Uso consapevole dell'utilizzo degli strumenti informatici e adeguata sensibilità ai temi della sicurezza informatica e della protezione dei dati personali
- Gestione delle credenziali di autenticazione (Password). Il collaboratore deve porre attenzione al fine di evitare la perdita delle stesse password e più in generale garantire la relativa segretezza
- Salvataggio dei dati in rete e non in locale (Desktop)
- Utilizzo dei protocolli di sicurezza informatica se presenti nella propria struttura (ad es. protocolli di cifratura, di pseudonimizzazione e anonimizzazione dei dati etc
- Limitazione nell'utilizzo dei supporti removibili e/o di altri supporti non "garantiti" da possibili virus e uso "prudente" di internet (evitare di navigare su siti poco raccomandabili)

REGOLE PER L'AUTORIZZATO AL TRATTAMENTO TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI INFORMATICI

- Mantenere l'assoluto riserbo sulle informazioni trattate all'interno della struttura
- Evitare di lasciare "liberi" sulle proprie scrivanie documenti al cui interno sono presenti dati personali
- Nei limiti del possibile evitare un accesso libero alle proprie stanze e/o uffici da parte di terzi non autorizzati.
- Rispettare i regolamenti interni e/o le disposizioni della direzione su chi possa fornire informazioni (ad esempio sanitarie e non) verso l'esterno.

REGIONE DEL VENETO
ULSS2 MARCA TREVIGIANA

Alcune questioni operative

Si possono dare informazioni sulla presenza dei pazienti nei reparti ?

A chi spetta la tenuta/conservazione della documentazione sanitaria (cartella clinica)?

Chi può dare informazioni sullo stato di salute al paziente oppure ai familiari?

E' possibile pubblicare sui social network/siti web le foto dei pazienti, "postare" documenti aziendali oppure fare commenti sui colleghi/Direzione?

LE RESPONSABILITÀ

Responsabilità civile

Chiunque subisca un danno materiale o immateriale a causa della violazione del Regolamento ha diritto di ottenere il risarcimento

REGIONE DEL VENETO
ULSS2 MARCA TREVIGIANA

Trattamento dati personali = Attività pericolosa

Chiunque subisca un danno materiale o immateriale causato da una violazione del regolamento ha il diritto di ottenere il risarcimento del danno dal titolare o dal responsabile del trattamento

Un titolare del trattamento risponde per il danno cagionato dal suo trattamento che violi il regolamento

Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare

Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile

Qualora più titolari o responsabili del trattamento siano coinvolti nello stesso trattamento e siano responsabili dell'eventuale danno causato dal trattamento, ogni titolare o responsabile è responsabile in solido per l'intero ammontare del danno con diritto di rivalsa

Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato

REGIONE DEL VENETO
ULSS2 MARCA TREVIGIANA

SANZIONI PENALI

Sebbene il GDPR si occupi principalmente di sanzioni amministrative,le sanzioni penali sono comunque considerate come uno strumento di ulteriore attuazioni e tutela delle nuova disciplina.
Spetterà agli Stati Membri prevedere tali sanzioni nel rispetto del principio che un soggetto non può essere processato e sanzionato per lo stesso reato.

REGIONE DEL VENETO
ULSS2 MARCA TREVIGIANA

SANZIONI AMMINISTRATIVE

Il Regolamento ha previsto solo le sanzioni massime, non quelle minime. Spetta al legislatore nazionale definire quest'ultime. In ogni caso si assisterà ad un inasprimento delle stesse

Fino a 10.000.000,00 euro
o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Fino a 20.000.000,00 euro
• o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.