Profili professionali relativi al trattamento e alla protezione dei dati personali

INDICE

SCHEDA REQUISITI (SK33)

PROCEDURA GESTIONALE (PD33)

SCHEDA REQUISITI

Definizione della figura professionale : la norma definisce i profili professionali relativi al trattamento e alla protezione dei dati personali.
Sono previsti 4 profili professionali:

- **RESPONSABILE PROTEZIONE DATI**
- **MANAGER PRIVACY**
- **SPECIALISTA PRIVACY**
- **VALUTATORE PRIVACY**

Conoscenze, abilità e competenze associate all'attività professionale: dal momento che la preparazione del professionista è globale e non segmentabile, ogni fase d'esame è costruita in modo tale da verificare sempre la completezza di conoscenze/abilità/competenze**.**

RESPONSABILE PROTEZIONE DATI

CONOSCENZE	ABILITA'	COMPETENZE
• I principi di privacy e protezione dei dati by design e by default I diritti degli interessati previsti da leggi e regolamenti vigenti Le responsabilità connesse al trattamento dei dati personali • Norme di legge italiane ed europee in materia di trattamento e di protezione dei dati personali • Norme di legge in materia di trasferimento di dati personali all'estero e circolazione dei dati personali extra UE/SEE • Le metodologie di valutazione d'impatto sulla protezione dei dati e PIA Le possibili minacce alla protezione dei dati personali • Le norme tecniche ISO/IEC per la gestione dei dati personali • I codici di condotta e le certificazioni applicabili in materia di trattamento e protezione dei dati personali • Tecniche e strumenti di comunicazione (relazione con Istituzioni, autorità, Forze dell'ordine, enti locali e stampa) • Le tecniche crittografiche • Le tecniche di anonimizzazione • Le tecniche di pseudonimizzazione • Sistemi e tecniche di monitoraggio e "reporting" • gli strumenti di controllo della versione per la produzione di documentazione K49 - i metodi di sviluppo delle competenze • i processi dell'organizzazione ivi inclusi le strutture decisionali, di budget e di gestione. • i rischi critici per la gestione della sicurezza • i tipici KPI (key performance indicators) • il potenziale e le opportunità offerte dagli standard e dalle best practices più rilevanti K85 - il ritorno dell'investimento comparato all'annullamento del rischio • l'impatto dei requisiti legali sulla sicurezza dell'informazione • la computer forensics (analisi criminologica di sistemi informativi) • la politica di gestione della sicurezza nelle aziende e delle sue implicazioni con gli impegni verso i clienti, i fornitori e i sub-contraenti • la strategia dell'informazione nell'organizzazione • le best practice (metodologie) e gli standard nella analisi del rischio K132 - le	• Contribuire alla strategia per il trattamento e per la protezione dei dati personali • Gestire l'applicazione dei codici di condotta e delle certificazioni applicabili in materia di trattamento e protezione dei dati personali • Capacità di comunicare Capacità di analisi • Autogestione e controllo dello stress • Capacità di autosviluppo Capacità di controllo Capacità di convincimento • Capacità di gestione dei conflitti • Iniziativa • Idoneità alla negoziazione • Capacità organizzative Pensiero prospettico • Pianificazione e programmazione • Atteggiamento costruttivo nella soluzione dei problemi • Tenacia • affrontare le esigenze della formazione continua (CPD) del personale per soddisfare le esigenze dell'organizzazione • analizzare gli asset critici dell'azienda ed identificare debolezze e vulnerabilità riguardo ad intrusioni o attacchi • anticipare i cambiamenti richiesti alla strategia aziendale dell'information security e formulare nuovi piani • applicare azioni di contenimento del rischio e dell'emergenza • applicare gli standard, le best practice e i requisiti legali più rilevanti all'information security • coaching • comunicare e pubblicizzare sia i risultati dell'analisi del rischio che i processi di gestione del rischio • comunicare le buone e le cattive notizie per evitare sorprese • costruire un piano di gestione del rischio per fornire e produrre piani di azione preventivi • garantire che la proprietà intellettuale (IPR) e le norme della privacy siano rispettate • identificare gap di competenze e skill gaps • negoziare termini e condizioni del contratto • preparare i template per pubblicazioni condivise • progettare e documentare i processi	• Pianificazione di Prodotto o di Servizio • Sviluppo della Strategia per la Sicurezza Informatica • Gestione del Contratto • Sviluppo del Personale • Gestione del Rischio • Gestione delle Relazioni • Gestione della Sicurezza dell'Informazione • Governance dei sistemi informativi

best practice e gli standard nella gestione della sicurezza delle informazioni K139 - le metodologie di analisi dei fabbisogni di competenze e skill • le norme legali applicabili ai contratti • e nuove tecnologie emergenti (per esempio sistemi distribuiti, modelli di virtualizzazione, sistemi di mobilità, data sets) • le possibili minacce alla sicurezza • le problematiche legate alla dimensione dei data sets (per esempio big data) • le problematiche relative ai dati non strutturati (per esempio data analytics) K180 - le tecniche di attacco informatico e le contromisure per evitarli	dell'analisi e della gestione del rischi • raccogliere la conoscenza interna ed esterna e i fabbisogni di informazione • rendere l'informazione disponibile • rispondere alle esigenze di sviluppo professionale del personale per soddisfare le esigenze organizzative • seguire e controllare l'uso effettivo degli standard documentativi aziendali • sviluppare piani di risk management per identificare le necessarie azioni preventive	

MANAGER PRIVACY

CONOSCENZE	ABILITA'	COMPETENZE
• l principi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita • I diritti degli interessati previsti da leggi e regolamenti vigenti • Le reti informatiche • Le reti di telecomunicazione • Le responsabilità connesse al trattamento dei dati personali • Norme di legge italiane ed europee in materia di trattamento e di protezione dei dati personali • Norme di legge in materia di trattamento e protezione dei dati personali nell'ambito delle comunicazioni elettroniche • Norme di legge in materia di trasferimento di dati personali all'estero e circolazione dei dati personali extra UE/SEE • Le metodologie di valutazione d'impatto sulla protezione dei dati e PIA Le possibili minacce alla protezione dei dati personali • Strumenti e metodi di pianificazione, programmazione e controllo aziendale Tecniche e strumenti di comunicazione (relazione con Istituzioni, autorità, Forze dell'ordine, enti locali e stampa) • Sistemi e tecniche di monitoraggio e "reporting' • codici di condotta e le certificazioni applicabili in materia di trattamento e protezione dei dati personali • DBMS, Data Warehouse. D55, ecc. • framework architetturali • framework architetturali, metodologie e strumenti per la progettazione di sistemi • gli standard della sicurezza ICT • gli strumenti di contrai° della versione per la produzione di documentazione • gli strumenti e gli apparati applicabili per la memorizzazione ed il recupero dei dati • gli strumenti per la creazione di presentazioni multimediali • gli strumenti per la produzione, l'editing e la distribuzione di documenti professionali • costi, benefici e rischi di un'architettura di sistema • i differenti documenti tecnici richiesti per la progettazione, lo sviluppo e il deploying dei prodotti, delle—applicazioni e dei servizi • i differenti modelli di servizio (SaaS, PaaS, laaS),	• Contribuire alla strategia per il trattamento e per la protezione dei dati personali • Gestire l'applicazione dei codici di condotta e delle certificazioni applicabili in materia di trattamento e protezione dei dati personali • Capacità di comunicare • Capacità di analisi • Autogestione e controllo dello stress Capacità di autosviluppo • Capacità di controllo • Capacità. di convincimento • Capacità di coordinamento e gestione dei collaboratori • Capacità decisionali • Flessibilità • Capacità di gestione dei conflitti • Capacità di gestione del gruppo • Iniziativa • Idoneità alla negoziazione • Capacità organizzative • Orientamento ai risultati • Pensiero prospettico • Pianificazione e programmazione • Atteggiamento costruttivo nella soluzione dei problemi • Tenacia • affrontare le esigenze della formazione continua (CPD) del personale per soddisfare le esigenze dell'organizzazione • analizzare gli asset critici dell'azienda ed identificare debolezze e vulnerabilità riguardo ad intrusioni o attacchi • analizzare gli sviluppi futuri nel processo di business e nell'applicazione della tecnologia • analizzare la fattibilità in termini di costi e benefici • applicare azioni di contenimento del rischio e dell'emergenza • applicare gli standard, le best practice e i requisiti legali più rilevanti all'information security • Coaching • collezionare, formalizzare e validare i requisiti funzionali e non funzionali • comprendere gli impatti delle nuove tecnologie sul business e come possono	• Pianificazione di Prodotto o di Servizio • Assistenza all'Utente • Progettazione di Architetture • Sviluppo della Strategia per la Sicurezza Informatica • Gestione del Contratto • Sviluppo del Personale • Gestione dell'Informazione e della Conoscenza • Gestione del Rischio • Gestione della Sicurezza dell'Informazione Governance dei Sistemi Informativi

livelli di servizio e contrattualizzazione degli stessi (per esempio Cloud Computing) • i metodi di sviluppo delle competenze • i metodi per lo sviluppo del software e la loro logica (per esempio prototipazione, metodi agili, reverse engineering, ecc.) • i principi della progettazione dell'interfaccia utente • i processi dell'organizzazione ivi inclusi le strutture decisionali, di budget e di gestione. • i rischi critici per la gestione della sicurezza • i tipici KPI (key performance indicators) • il potenziale e le opportunità offerte dagli standard e dalle best practices più rilevanti, • il ritorno dell'investimento comparato all'annullamento del rischio • l'impatto dei cambiamenti del business sugli aspetti legali • l'impatto dei requisiti legali sulla sicurezza dell'informazione • l'infrastruttura ICT e l'organizzazione del business • la computer forensics (analisi criminologica di sistemi informativi) • la politica di gestione della sicurezza nelle aziende e delle sue implicazioni • con gli impegni verso i clienti, i fornitori e i sub-contraenti • la strategia dell'informazione nell'organizzazione • le applicazioni esistenti e le relative architetture • le applicazioni ICT utente rilevanti • le best practice (metodologie) e gli standard nella analisi del rischio • le best practice e gli standard nella gestione della sicurezza delle informazioni • le metodologie di analisi dei fabbisogni di competenze e skill • le norme legali applicabili ai contratti • le nuove tecnologie emergenti (per esempio sistemi distribuiti, modelli di virtualizzazione, sistemi di mobilità, data sets) • le possibili minacce alla sicurezza • le problematiche legate alla dimensione dei data sets (per esempio big data) • le problematiche relative ai dati non strutturati (per esempio data analytics) • le strategie digitali • le tecniche di attacco informatico e le contromisure per evitarli • le tecniche di rilevamento di sicurezza, compreso il mobile e il digitale • le tecnologie web, cloud e mobile • le tendenze e le implicazioni dello sviluppo interno o esterno dell'ICT nelle organizzazioni tipiche • requisiti dell'architettura dei sistemi: prestazioni, manutenibilità, estendibilità, scalabilità, disponibilità, sicurezza e accessibilità	fornire valore e vantaggio competitivo (per esempio open i big data. dematerializzazione opportunità e strategie) • comprendere gli obiettivi / elementi guida del business che impattano i componenti dell'architettura (dati, applicazioni, sicurezza, sviluppo, ecc.). • comprendere il contesto giuridico e normativo per integrarlo nelle esigenze di business • comprendere le architetture di impresa • comunicare chiaramente con l'utente finale e fornire istruzioni sui progressi nella soluzione dei problemi • comunicare e pubblicizzare sia i risultati dell'analisi del rischio che i processi di gestione del rischio • comunicare il valore, i rischi e le opportunità derivanti dalla strategia del sistema informativo • comunicare le buone e le cattive notizie per evitare sorprese • contribuire allo sviluppo della strategia di business • contribuire allo sviluppo della strategia e delle politiche dell'ICT, incluse la qualità e la sicurezza ICT • costruire un piano di gestione del rischio per fornire e produrre piani di azione preventivi • definire ed implementare adeguati key performance indicators (KPI's) • garantire che la proprietà intellettuale (IPR) e le norme della privacy siano rispettate • negoziare termini e condizioni del contratto • preparare i template per pubblicazioni condivise • progettare e documentare i processi dell'analisi e della gestione del rischio • proporre misure efficaci di contingenza • raccogliere la conoscenza interna ed esterna e i fabbisogni di informazione • rendere l'informazione disponibile • seguire e controllare l'uso effettivo degli standard documentativi aziendali • selezionare soluzioni iCT appropriate basandosi su benefici attesi, rischi ed impatto complessivo • stabilire un piano di ripristino • stabilire una comunicazione sistematica e frequente con i clienti, gli utenti e gli stakeholder • sviluppare modelli e pattern per assistere gli analisti di sistema nella progettazione di applicazioni consistenti • sviluppare piani di risk management per identificare le necessarie azioni preventive valutare l'idoneità di differenti metodi di sviluppo dell'applicazione rispetto allo scenario corrente	

SPECIALISTA PRIVACY

CONOSCENZE	ABILITA'	COMPETENZE
• I principi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita • I diritti degli interessati previsti da leggi e regolamenti vigenti • Le reti informatiche • Le reti di telecomunicazione • Le responsabilità connesse al trattamento dei dati personali • Norme di legge italiane ed europee in materia di trattamento e protezione dei dati personali con particolare riguardo alle disposizioni di rango primario e secondario (regolamenti, provvedimenti, autorizzazioni, linee-guida e standard settoriali, altro) relative agli specifici ambiti di operatività • Norme di legge in materia di trattamento e protezione dei dati personali nell'ambito delle comunicazioni elettroniche • Norme di legge in materia di trattamento e protezione dei dati personali per finalità di videosorveglianza • Norme di legge in materia di trattamento e protezione dei dati personali per finalità di marketing e profilazione • Norme di legge in materia di trattamento e protezione dei dati personali per finalità di controllo dei lavoratori • Norme di legge in materia di trasferimento di dati personali all'estero e circolazione dei dati personali extra UEISEE • Norme di legge per la gestione di dati biometrici • Impiantistica di videosorveglianza • Le metodologie di valutazione d'impatto sulla protezione dei dati e PIA • Le possibili minacce alla protezione dei dati personali con riguardo, in particolare, allo specifico settore di operatività • Le tecniche crittografiche • Le tecniche di anonimizzazione e de-anonimizzazione • Le tecniche di pseudorfimizzazione • Le tecnologie loT (Internet of Things) • Le tecnologie R Fl D • Le tecnologie di geolocalizzazione • Le tecnologie di identificazione • Le tecnologie di identificazione biometriche • Le tecnologie di tracciamento delle operazioni • I codici di condotta e le certificazioni applicabili in materia di trattamento e protezione dei dati personali • DBMS, Data Warehouse, DSS, ecc. • framework architetturali, metodologie	• Applicare i principi di privacy e protezione dei dati by design e by default ai sistemi informativi • Applicare i principi di privacy e protezione dei dati by design e by default ai trattamenti di dati personali • Gestire le richieste da parte degli interessati che esercitano i loro diritti • Elaborare procedure di trasferimento soggetto a garanzie adeguate e/o norme vincolanti d'impresa verso paesi terzi od organizzazioni internazionali • Capacità di lavoro in gruppo • Capacità di analisi • Flessibilità • Capacità organizzative • Pianificazione e programmazione • Propensione al nuovo • affrontare le esigenze della formazione continua (CPD) del personale per soddisfare le esigenze dell'organizzazione • analizzare gli asset critici dell'azienda ed identificare debolezze e vulnerabilità riguardo ad intrusioni o attacchi • analizzare l'impatto sugli utenti dei cambiamenti funzionaiiitecnici • anticipare i cambiamenti richiesti alla strategia aziendale dell'information security e formulare nuovi piani • anticipare tutte le azioni necessarie a mitigare l'impatto dei cambiamenti (formazione, documentazione, nuovi processi...) • applicare azioni di contenimento del rischio e dell'emergenza • applicare metodi di data mining • capire come le tecnologie web possono essere utilizzate per il marketing • coaching • collezionare, formalizzare e validare i requisiti funzionali e non funzionali • comporre. ddcumentare e classificare i processi fondamentali e le procedure • comprendere gli obiettivi/elementi guida del business che impattano i componenti dell'architettura (dati, applicazioni, sicurezza, sviluppo, ecc.) • comunicare chiaramente con l'utente finale e fornire istruzioni sui progressi nella soluzione dei problemi • condividere specifiche funzionali e tecniche con i team ICT che hanno in carico la manutenzione e l'evoluzione delle soluzioni ICT • garantire che controlli e funzionalità vengano recepiti dalla progettazione • garantire che la proprietà intellettuale (IPR) e le norme della privacy siano rispettate • preparare i template per pubblicazioni condivise • raccogliere la conoscenza interna ed esterna e i fabbisogni dí informazione • raccogliere, immagazzinare, analizzare data sets complessi larghi non strutturati e in formati differenti	• Progettazione di Architetture • Progettazione di Applicazioni • Produzione di documentazione • Assistenza all'utente • Supporto alle modifiche/evoluzioni di sistema • Sviluppo del Personale • Gestione dell'Informazione e della Conoscenza • Gestione del Rischio • Gestione della Sicurezza dell'Informazione

e strumenti per la progettazione di sistemi • gli strumenti di controllo della versione per la produzione di documentazione • gli strumenti e gli apparati applicabili per la memorizzazione ed il recupero dei dati • gli strumenti per la creazione di presentazioni multimediali • gli strumenti per la produzione, l'editing e la distribuzione di documenti professionali • i costi, benefici e rischi di un'architettura di sistema • i differenti documenti tecnici richiesti per la progettazione, lo sviluppo e il • deploying dei prodotti, delle applicazioni e dei servizi • i metodi di sviluppo delle competenze • i metodi per analizzare le informazioni non strutturate e i processi di business • i metodi per lo sviluppo del software e la loro logica (per esempio • prototipazione, metodi agili, reverse engineering, ecc.) • i principi della progettazione dell'interfaccia utente • il mobile marketing (per esempio Pay Per Click) • il social media marketing • l'architettura tecnica di un'applicazione ICT esistente • ['e-mail marketing • la computer forensics (analisi criminologica di sistemi informativi) • le applicazioni esistenti e le relative architetture • le best practice e gli standard nella gestione della sicurezza delle informazioni • le nuove tecnologie emergenti (per esempio sistemi distribuiti, modelli di • virtualizzazione, sistemi di mobilità, data sets) • le problematiche legate alla dimensione dei data sets (per esempio big data) • le problematiche relative ai dati non strutturati (per esempio data analytics) • le specifiche funzionali di un sistema informativo • le strutture del database e l'organizzazione dei suoi contenuti • le tecniche di attacco informatico e le contromisure per evitarli • le tecniche di rilevamento di sicurezza, compreso il mobile e il digitale • le tecnologie web, cloud e mobile • requisiti dell'architettura dei sistemi: prestazioni, manutenibilità, estendibilità. scalabilità, disponibilità, sicurezza e accessibilità	• rendere l'informazione disponibile • seguire e controllare l'uso effettivo degli standard documentativi aziendali • stabilire una comunicazione sistematica e frequente con i clienti, gli utenti e -gli stakeholder • sviluppare modelli e pattern per assistere gli analisti di sistema nella progettazione di applicazioni consistenti • usare e analizzare la web analytics • valutare l'idoneità di differenti metodi di sviluppo dell'applicazione rispetto allo scenario corrente	

VALUTATORE PRIVACY

CONOSCENZE	ABILITA'	COMPETENZE
• I principi di protezione dei dati fin dalla	• Verificare l'applicazione dei principi di	• Progettazione di architetture

progettazione e di protezione per impostazione predefinita • I diritti degli interessati previsti da leggi e regolamenti vigenti • Norme di legge italiane ed europee in materia di trattamento e di protezione dei dati personali • Norme di legge in materia di trattamento e protezione dei dati personali nell'ambito delle comunicazioni elettroniche • Norme di legge in materia di trattamento e protezione dei dati personali per finalità di videosorveglianza • Norme di legge in materia di trattamento e protezione dei dati personali per finalità di marketing e profilazione • Norme di legge in materia di trattamento e protezione dei dati personali per finalità di controllo dei lavoratori • Norme di legge in materia di trasferimento di dati personali all'estero e circolazione dei dati personali extra UE/SEE • Norme di legge per la gestione di dati biometrici • Impiantistica di videosorveglianza • Le metodologie di valutazione d'impatto sulla protezione dei dati e PIA Le possibili minacce alla protezione dei dati personali • Le tecniche crittografiche • Le tecniche di anonimizzazione e de-anonimizzazione • Le tecniche di pseudonimizzazione • Le tecnologie loT (Internet of Things) • Le tecnologie RFID • Le tecnologie di geolocalizzazione • Le tecnologie di identificazione • Le tecnologie di identificazione biometriche • Le tecnologie di tracciamento delle operazioni • Le norme tecniche ISO/IEC per la gestione dei dati personali • Le best practice (metodologie) e gli standard per l'auditing e per l'accreditamento I codici di condotta e le certificazioni applicabili in materia di trattamento e protezione dei dati personali • Capacità di lavoro in gruppo • Accuratezza • Capacità di analisi • Pianificazione e programmazione • Capacità di sintesi • DBMS, Data Warehouse. DSS, ecc. • framework architetturali, metodologie e strumenti per la progettazione di sistemi • gli strumenti di controllo della versione per la produzione di documentazione • gli strumenti e gli apparati applicabili per la memorizzazione ed il recupero	protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita • Capacità di lavoro in gruppo • Accuratezza • Capacità di analisi • Pianificazione e programmazione • Capacità di sintesi • analizzare gli asset critici dell'azienda ed identificare debolezze e vulnerabilità riguardo ad intrusioni o attacchi • applicare gli standard, le test practioe e i requisiti legali più rilevanti all'informalion security • applicare metodi di data mining • collezionare, formalizzare e validare i requisiti funzionali e non funzionali S45 - comporre, documentare e classificare i processi fondamentali e le procedure • comprendere gli obiettivi I elementi guida del business che impattano i componenti dell'architettura (dati, applicazioni, sicurezza, sviluppo, ecc.) • garantire che la proprietà intellettuale (IPR) e le norme della privacy siano rispettate • rendere l'informazione disponibile • seguire e controllare l'uso effettivo degli standard documentativi aziendali	• Progettazione di applicazioni • Produzione della documentazione • Gestione dell'informazione e della Conoscenza • Gestione del Rischio • Miglioramento del processo • Gestione della sicurezza dell'informazione

dei dati • gli strumenti per la creazione di presentazioni multimediali • gli strumenti per la produzione, l'editing e la distribuzione di documenti professionali • i costi, benefici e rischi di un'architettura di sistema • i differenti documenti tecnici richiesti per la progettazione, Io sviluppo e il deploying dei prodotti, delle applicazioni e dei servizi • i metodi per analizzare le informazioni non strutturate e i processi di business • i metodi per lo sviluppo del software e la loro logica (per esempio prototipazione, metodi agili, reverse engineering, ecc.) • i principi della progettazione dell'interfaccia utente • i rischi critici per la gestione della sicurezza • il potenziale e le opportunità offerte dagli standard e dalle best practice più rilevanti. • l'approccio all'auditing interno del sistema informativo • l'impatto dei cambiamenti del business sugli aspetti legali • l'impatto dei requisiti legali sullasicurezza dell'informazione • le best practice (metodologie) e gli standard nella analisi del rischio • le best practice e gli standard nella gestione della sicurezza delle informazioni • le norme legali applicabili ai contratti • le possibili minacce alla sicurezza • le problematiche legate alla dimensione dei data sets (per esempio big data) • le problematiche relative ai dati non strutturati (per esempio data analytics) • le tecniche di rilevamento di sicurezza, compreso il mobile e il digitale • le tecnologie web, cloud e mobile • requisiti dell'architettura dei sistemi: prestazioni, manutenibilità, estendibilità. • scalabilità, disponibilità, sicurezza e accessibilità		

Requisiti minimi di certificazione:

Cat.	Skills	Requisiti minimi	Note/osservazioni
A	**Titolo di studio**	• **RESPONSABILEE PROTEZIONE DATI e/o MANAGER PRIVACY** : laurea che includa discipline almeno in parte afferenti alle conoscenze del professionista privacy, legali o tecnico/informatiche • **SPECIALISTA PRIVACY e/o VALUTATORE PRIVACY**: Diploma di scuola media superiore	Sono accettati tutti i titoli, corsi e diplomi riconosciuti equipollenti a quelli italiani, ai sensi delle vigenti disposizioni di legge. Un laureato con laurea non afferente alle conoscenze del professionista privacy, legali o tecnico/informatiche è da equipararsi al diplomato di scuola media superiore

A/1	**Formazione specifica**	• **RESPONSABILE PROTEZIONE DATI:** corso di almeno 80 ore • **MANAGER PRIVACY:** Corso di almeno 60 ore • **SPECIALISTA PRIVACY:** corso di almeno 24 ore • **VALUTATORE PRIVACY:** corso di almeno 40 ore	FAC CERTIFICA provvederà a valutare, tramite specifica commissione, la congruità delle ore di formazione prodotte, con la professione svolta Il corso dovrà avere per argomento la gestione della privacy e della sicurezza delle informazioni E' ammissibile la riduzione delle ore di formazione richieste fino ad un massimo del 10% (30% per il VALUTATORE) in caso di possesso di certificazioni professionali riconosciute come attinenti alle conoscenze richieste al professionista privacy in questione.
B	**Esperienza di lavoro specifica** E' necessaria una documentata ed appropriata esperienza lavorativa specifica nell'ambito Privacy presso strutture pubbliche, private o come libero professionista	• **RESPONSABILE PROTEZIONE DATI:** Minimo 6 anni di esperienza lavorativa legata alla privacy di cui almeno 4 anni in incarichi di livello manageriale	EQUIPOLLENZA: Se in possesso di laurea magistrale l'esperienza lavorativa si riduce a 4 anni di cui 3 in incarichi di livello manageriale. Se in possesso di diploma di scuola media superiore minimo 8 anni di esperienza lavorativa di privacy di cui almeno 5 anni in incarichi di livello manageriale.
		• **MANAGER PRIVACY:** Minimo 6 anni di esperienza lavorativa legata alla privacy di cui almeno 3 anni in incarichi di livello manageriale	EQUIPOLLENZA: Se in possesso di laurea magistrale l'esperienza lavorativa si riduce a 4 anni di cui 2 in incarichi di livello manageriale. Se in possesso di diploma di scuola media superiore minimo 8 anni di esperienza lavorativa di privacy di cui almeno 4 anni in incarichi di livello manageriale.
		• **SPECIALISTA PRIVACY:** Minimo 4 anni di esperienza lavorativa legata alla privacy	EQUIPOLLENZA: Se in possesso di laurea l'esperienza lavorativa si riduce a 2 anni.
		• **VALUTATORE PRIVACY:** Minimo 6 anni di esperienza lavorativa continuativa legata alla privacy di cui almeno 3 anni in incarichi di audit	EQUIPOLLENZA: Se in possesso di laurea l'esperienza lavorativa si riduce a 4 anni di cui 2 in incarichi di audit. Se in possesso di Laurea Magistrale minimo 3 anni di esperienza lavorativa di cui 2 in incarichi di audit.
C	**Esame**	**Superamento di Esame di Certificazione**	
	<u>Esame on-line e/o in presenza</u> C.1 Prova Scritta C.2 Prova Scritta C.3 Prova Orale	**C.1** Test conoscitivo basato sullo schema ottimale di competenze Privacy **C.2** Caso di studio con risposta aperta **C.3** Intervista	Per le modalità di attuazione e superamento dell'esame vedere allegata PD33 (pag 7. e segg.)
D	**Valutazione**		
	D.1 Valutazione delle competenze	La valutazione avviene secondo la procedura (PD33), vigente, a seguito del superamento dell'esame in presenza di commissione o, a scelta del candidato, on-line	I commissari devono essere certificati o selezionati da FAC CERTIFICA.
	D.2 Criteri di valutazione	I criteri di valutazione saranno espressi da indicatori numerici (crediti) secondo quanto dettagliato nella procedura (PD33) vigente	I criteri di valutazione sono distribuiti nelle 3 aree specifiche di: ▪ Conoscenze ▪ Abilità

			▪ Caratteristiche personali
	D.3 Esito della valutazione	La valutazione complessiva tiene conto di tutti i requisiti richiesti e delle prove di esame e viene sottoposta agli organi FAC CERTIFICA competenti per il rilascio della certificazione.	
E	**Iscrizione al registro**	Il candidato che supera l'esame e dimostra di possedere tutti i requisiti della presente scheda viene iscritto nel registro FAC CERTIFICA e riceve il certificato e il timbro attestanti il possesso della certificazione.	Il registro dei Professionisti certificati è visibile sul sito FAC CERTIFICA: www.faccertifica.it
F	**Durata**	La durata della certificazione di conformità alla norma UNI 11697:2017 è triennale e si rinnova, in assenza di revoca e/o rinuncia, al termine dei tre anni di validità	

Requisiti per il mantenimento annuale della certificazione

Cat.	Requisiti	Evidenze	Note/osservazioni
A	**Deontologia professionale**	Nessuna segnalazione negativa in merito al rispetto del Regolamento di Certificazione del Personale FAC CERTIFICA	Compilazione del Mod. 'MO09' rev.00
B	**Corretto utilizzo Certificazione**	Nessuna segnalazione negativa in merito al rispetto del Regolamento di Certificazione del Personale FAC CERTIFICA	Compilazione del Mod. 'MO09' rev.00
C	**Reclami**	Assenza	Compilazione del Mod. 'MO09' rev.00
D	**Quota annuale di mantenimento**	Assolta	Confrontare il sito www.faccertifica.it sezione "Tariffario"
E	**Aggiornamento professionale**	- partecipazione come relatore ad almeno due convegni afferenti a temi rispettivamente di trattamento e di protezione dei dati; oppure - superamento di un corso di aggiornamento sui temi afferenti rispettivamente al trattamento o alla protezione dei dati della durata minima di 8 ore (aumentate a 16 ore e non sostituibile dagli altri punti qui riportati per il Responsabile della protezione dati); oppure - avere svolto, in tema rispettivamente di trattamento o di protezione dei dati, attività di docenza oppure pubblicato articoli o testi afferenti ai temi sopra illustrati; leggere con regolarità bollettini e pubblicazioni in materia di protezione dei dati personali. La documentazione della lettura di tali testi deve esser	- Evidenza della partecipazione: attestati, doc.ti di iscrizione, fatture. Ad ogni ora di partecipazione verrà attribuito 1 HPCD[1] - A titolo esemplificato, ma non esaustivo, per aggiornamento si intende la partecipazione a corsi, convegni e seminari su tematiche attinenti, in qualità di discente e/o docente - Gli aggiornamenti possono essere effettuati in aula e/o on-line - Compilazione del modulo "MO09"

[1] HHCPD: Hours of Continuing Professional Development

		supportata da elementi oggettivi, connessi per esempio alla durata del tempo dedicato alla lettura di tali testi.	

Requisiti per il rinnovo triennale: per mantenere il livello medio-alto che i professionisti devono dimostrare di avere per ottenere la certificazione, dal momento che le professioni sono soggette ad un'obsolescenza rapida, è sufficiente effettuare l'aggiornamento professionale richiesto. Non si ravvisa quindi la necessità di far svolgere ulteriori esami ai professionisti per il rinnovo della certificazione.

Cat.	Requisiti	Evidenze	Note/osservazioni
A	**Deontologia professionale**	Nessuna segnalazione negativa in merito al rispetto del Regolamento di Certificazione del Personale FAC CERTIFICA	Compilazione del Mod. 'MO10' rev.00
B	**Corretto utilizzo Certificazione**	Nessuna segnalazione negativa in merito al rispetto del Regolamento di Certificazione del Personale FAC CERTIFICA	Compilazione del Mod. 'MO10' rev.00
C	**Reclami**	Assenza	Compilazione del Mod. 'MO10' rev.00
D	**Quota annuale di mantenimento**	Assolta	Confrontare il sito www.faccertifica.it sezione "Tariffario"
E	**Continuità professionale**	Documentata ed appropriata esperienza lavorativa continuativa specifica con cui si è svolta l'attività nell'arco dei tre anni di durata del Certificato	Compilazione del Mod. 'MO10' rev.00
F	**Aggiornamento professionale**	Quanto previsto annualmente per il mantenimento, dalla norma UNI 11697 Qualora, al termine del triennio, il professionista non fosse riuscito ad effettuare tutte le ore di aggiornamento richieste, è prevista la possibilità di effettuare un prova scritta (test) on-line, al fine di mantenere la certificazione	- Evidenza della partecipazione: attestati, doc.ti di iscrizione, fatture. Ad ogni ora di partecipazione verrà attribuito 1 HPCD[1] - A titolo esemplificato, ma non esaustivo, per aggiornamento si intende la partecipazione a corsi, convegni e seminari su tematiche attinenti, in qualità di discente e/o docente - Gli aggiornamenti possono essere effettuati in aula e/o on-line - Compilazione del Mod. 'MO10' rev.00

PROCEDURA GESTIONALE

SCOPO E CAMPO DI APPLICAZIONE: La presente procedura descrive le modalità operative adottate da FAC CERTIFICA per l'attività di valutazione e certificazione dei Profili professionali relativi al trattamento e alla protezione dei dati personali

RIFERIMENTI: Riferimenti normativi utilizzati da FAC CERTIFICA per la certificazione dei Profili professionali relativi al trattamento e alla protezione dei dati personali

Manuale del Sistema di Gestione per la Qualità FAC CERTIFICA		**MN01**
Schema di Certificazione FAC CERTIFICA:	Regolamento Generale	**RL01**
	Modulo richiesta ammissione esame	**MO03** (esame in presenza di commissione) **MO04** (esame on-line)
	Scheda Requisiti	**SK 33**
	Procedura gestionale	**PD 33**
Norma UNI CEI EN ISO/IEC 17024:2012		
Norma UNI 11697:2017		
D.lgs 196/2003		
Reg. UE 679/2016		
Direttiva UE 680/2016		

PROCESSO DI VALUTAZIONE: La valutazione di idoneità del Candidato, ai fini del rilascio della certificazione FAC CERTIFICA, avviene attraverso la sequenza, temporale e vincolante, di ciascuna delle seguenti fasi:

	FASI:		NOTE/OSSERVAZIONI
1.	valutazione preliminare della documentazione prodotta dal Candidato	il Direttore FAC CERTIFICA, con l'ausilio del personale dipendente, effettua una valutazione preliminare della documentazione prodotta, al fine di verificare il possesso o meno dei requisiti minimi di cui alla Scheda SK33 che devono essere supportati dalla documentazione e confermate da un numero minimo di evidenze	Il commissario effettua un'ulteriore analisi documentale per valutarne l'adeguatezza e verificare eventuali situazioni che possano bloccare l'ammissione all'esame
2.	esame FAC CERTIFICA per la valutazione dei candidati	Esame condotto a fronte di parametri e sulla base di strumenti prefissati, specificati nel paragrafo successivo;	La valutazione delle prove d'esame è a cura del/i commissario/i, nominato da FAC CERTIFICA
3.	valutazione tecnica dei risultati, di cui ai punti sopra indicati, eseguita dal Comitato di Delibera FAC CERTIFICA	La valutazione è eseguita dal Comitato di Delibera FAC CERTIFICA	
4.	delibera	La delibera è a cura del Comitato di Delibera FAC CERTIFICA	Qualora l'esito di una qualsiasi delle suddette fasi sia negativo, FAC CERTIFICA interrompe il processo di valutazione e informa il Candidato che decide quindi se proseguire o meno nell'iter di certificazione. Per procedere nell'iter sarà necessario prima risolvere le carenze riscontrate nella singola fase, nei tempi indicati da FAC CERTIFICA.

ESAME: *sono previste due tipologie d'esame: in presenza di commissione ed on-line.*
Sono ammessi a sostenere l'esame FAC CERTIFICA tutti coloro che, avendo presentato formale richiesta, attraverso il modulo (MO03/MO04), documentano il possesso dei seguenti requisiti minimi, allegandoli al modulo e di cui alla Scheda SK33

ESAME ON-LINE	Requisiti minimi da allegare al modulo di iscrizione	Note/osservazioni
1	Diploma di Scuola Secondaria Superiore o Laurea	Cfr. pag. 3-4, *"Requisiti minimi di certificazione" sez.Titolo di studio* Inviare copia del titolo di studio o autocertificazione
2	Evidenze oggettive in merito all'esperienza lavorativa specifica nel campo	Cfr. pag 3 - 4, *"Requisiti minimi di certificazione"sez. Esperienza di lavoro specifica.* A titolo esemplificativo, ma non esaustivo, possono essere inviate, quali evidenze: dichiarazioni del datore di lavoro o di clienti, contratti di lavoro, certificato attribuzione P.IVA, esempi di fatture emesse prive dei dati sensibili, visure camerali ecc.
3	Formazione specifica	Allegare copia dell' attestato/i del corso/i
4	Copia documento di identità	Sono accettati: carta di identità, passaporto, patente di guida.
5	Curriculum vitae	Deve essere in formato europeo, firmato, datato e con l'autorizzazione al trattamento dei dati personali (D.Lgs.196/03)
6	Regolamento FAC CERTIFICA (RL01)	Il regolamento è scaricabile sul sito www.faccertifica.it/it/certificazione/modulisticaperesami/ Deve essere spedita unicamente l'ultima pagina, datata e firmata per accettazione
7	Fotografia	La fotografia serve ad identificare l'identità del candidato. Deve perciò essere recente. Può essere integrata all'interno del curriculum vitae o allegata a parte
8	Computer	Requisiti minimi: *sistema operativo:* • Mac OSX >= 10.7.5 Lion • Windows XP SP2 o superiore *Browser:* • Mozilla Firefox (versione 18 o seguenti)
9	Web-cam	Può essere integrata nel computer od esterna e la sua funzionalità è vincolante per l'accesso all'esame
10	regolare pagamento della quota prevista per l'ammissione all'esame	Cfr. TARIFFARIO FAC CERTIFICA su http://www.faccertifica.it/it/certificazione/tariffario/ *Sez. esami on-line.* La quota di iscrizione comprende la possibilità di effettuare 3 prove d'esame nell'arco di 4 mesi.

ESAME IN PRESENZA DI COMMISSIONE	Requisiti minimi da allegare al modulo di iscrizione	Note/osservazioni
1	Diploma di Scuola Secondaria Superiore o Laurea	Cfr. pag 3-4, *"Requisiti minimi di certificazione" sez.Titolo di studio* Inviare copia del titolo di studio o autocertificazione
2	Evidenze oggettive in merito all'esperienza lavorativa specifica nel campo	Cfr. pag 3-4, *"Requisiti minimi di certificazione"sez. Esperienza di lavoro specifica.* A titolo esemplificativo, ma non esaustivo, possono essere inviate, quali evidenze: dichiarazioni del datore di lavoro o di clienti, contratti di lavoro, certificato attribuzione P.IVA, esempi di fatture emesse prive dei dati sensibili, visure camerali ecc.)
3	Formazione specifica	Allegare copia dell' attestato/i del corso/i
4	Copia documento di identità	Sono accettati: carta di identità, passaporto, patente di guida.
5	Curriculum vitae	Deve essere in formato europeo, firmato, datato e con l'autorizzazione al trattamento dei dati personali (D.Lgs.196/03)
6	Regolamento FAC CERTIFICA (RL01)	Il regolamento è scaricabile sul sito www.faccertifica.it/it/certificazione/modulisticaperesami/ Deve essere spedita unicamente l'ultima pagina, datata e firmata per accettazione
7	regolare pagamento della	Cfr. TARIFFARIO FAC CERTIFICA su

	quota prevista per l'ammissione all'esame	http://www.faccertifica.it/it/certificazione/tariffario/ *Sez. esami in presenza di commissione* La quota di iscrizione è relativa ad ogni sessione d'esame

FINALITÀ DELL' ESAME:

1) approfondire nell'ambito dell'esperienza professionale le informazioni presentate dal Candidato	valutazione del grado di adeguatezza della documentazione e dei titoli presentati e la loro congruenza con la certificazione richiesta;	tale valutazione viene effettuata a cura del commissario/i d'esame
2) accertare il possesso da parte del Candidato delle conoscenze tecniche e metodologiche necessarie a svolgere con competenza la professione ai fini del rilascio della relativa Certificazione	Rientrano tra tali conoscenze e abilità gli argomenti indicati nella sez. *"Conoscenze, abilità e competenze associate all'attività professionale"* a pag . 3	L'esame è condotto dai Commissari d'esame FAC CERTIFICA , nominati dal Direttore e scelti nell'elenco FAC CERTIFICA dei commissari. I Commissari sono responsabili della valutazione delle prove d'esame del Candidato e per questo ne rispondono a FAC CERTIFICA; per tutte le attività di valutazione i Commissari garantiscono indipendenza di giudizio, assenza di conflitto di interessi e riservatezza dei dati.

MODALITÀ SVOLGIMENTO ESAME, ARGOMENTI, E CRITERI DI VALUTAZIONE

ESAME ON_LINE		**Note/Osservazioni**
Modalità di svolgimento	L'esame FAC CERTIFICA si svolge mediante accesso riservato on-line al sito unc.it/linkomm/fac/facquiz.php	Il candidato accede all'area d'esame tramite password e login che il Direttore, con l'ausilio del personale dipendente, provvede a comunicare a ciascun candidato. L'identità del candidato viene monitorata durante tutta la prova d'esame tramite web-cam
Argomenti	L'esame on-line è composto da 3 parti:	Per gli argomenti d'esame confrontare pag 3 *"Conoscenze, abilità e competenze associate all'attività professionale"*
	1) <u>test scritto</u> composto da domande a risposta chiusa (ossia 1 sola risposta di quelle presentate è vera). A positivo superamento di questa prova,	Il test scritto prevede 30 domande, con 3 risposte ciascuna ed è previsto un tempo massimo di 30 minuti (90 secondi per ogni domanda). Durante l'intero svolgimento della prova d'esame, il Candidato non può consultare alcun tipo di materiale didattico L'esito della prova è immediato.
	2) <u>"caso di studio"</u> : viene proposta una situazione reale, attinente alla specifica attività professionale, a cui il Candidato dovrà fornire una risposta appropriata A positivo superamento di questa prova,	Il caso di studio prevede un tempo massimo di risposta di 30 minuti. Durante l'intero svolgimento della prova d'esame, il Candidato non può consultare alcun tipo di materiale didattico La risposta fornita dal candidato viene inviata al/i commissario/i, nominato da FAC CERTIFICA
	3) <u>esame orale</u>, tramite videoconferenza	L'esame orale è volto ad approfondire eventuali incertezze riscontrate nelle prove scritte e/o per approfondire il livello delle conoscenze acquisite dal candidato ed è condotto da un commissario

		nominato da FAC CERTIFICA .Per tale prova è previsto un tempo massimo di 20 minuti
Criteri di valutazione	La valutazione massima ottenibile è di 100 punti, ed è data dalla sommatoria delle votazioni conseguite dal candidato nelle 3 prove d'esame La valutazione complessiva è positiva se la somma delle votazioni ottenute nelle tre prove (2 scritte e 1 orale) raggiunge almeno 60 punti, tenendo comunque presente che deve essere superata la soglia minima fissata per ogni prova: per la prima prova scritta 18 punti, per la seconda prova scritta 18 punti e per la terza prova orale 24 punti.	
		Prima prova (test): viene attribuita una votazione massima di 30 punti: 1 punto per ogni risposta corretta, 0 punti per ogni risposta sbagliata o non assegnata Seconda prova (caso di studio): viene attribuito un punteggio massimo di 30 punti. Terza prova (orale): viene attribuita una votazione massima di 40 punti
Esito negativo esame	Nel caso di non superamento dell' esame il candidato avrà a sua disposizione altri 2 tentativi con modalità on-line	La quota di iscrizione all'esame on-line prevede 3 tentativi d'esame, senza ulteriori esborsi economici, nell' arco di 4 mesi a far data dalla comunicazione della password di accesso all'area riservata.
Esito positivo esame e Rilascio della certificazione	Il Candidato che dimostra il possesso di tutti i requisiti richiesti ed ha superato positivamente l'esame, viene proposto dal Direttore al Comitato di Delibera FAC CERTIFICA. Il Comitato di Delibera valuta, sulla base di tutta la documentazione relativa al Candidato, il possesso dei requisiti e può riservarsi di accertare, ulteriormente, il possesso delle caratteristiche personali attraverso opportune tecniche (p.es. intervista, richiesta di documentazione aggiuntiva) ed eventuali informazioni da richiedere alle strutture presso cui, o per conto delle quali, il Candidato ha eseguito prestazioni. In tal caso, il Comitato stabilisce anche quali tempi e modalità siano necessari. Il Comitato di Delibera si riserva inoltre di valutare ulteriormente la congruenza tra la documentazione presentata dal Candidato, la valutazione effettuata dai commissari d'esame e la proposta di certificazione. Ad esito positivo della valutazione, il Comitato delibera per il rilascio della certificazione. La notifica dell'ottenimento della certificazione, unitamente alle modalità per la consegna di certificato, vengono comunicate al Candidato dal Direttore con l'ausilio del personale FAC CERTIFICA	

ESAME IN PRESENZA DI COMMISSIONE		**Note/Osservazioni**
Modalità di svolgimento	L'esame FAC CERTIFICA si svolge nelle località e date stabilite, di volta in volta, dal Direttore il quale, con l'ausilio del	Alla sessione d'esame FAC CERTIFICA sono presenti i candidati, la Commissione d'esame e il personale FAC CERTIFICA.

	personale dipendente, provvede a comunicarle a ciascun Candidato.	Prima dell'inizio delle prove d'esame, i candidati sono tenuti a: - esibire un documento di identità valido, - firmare il foglio presenze
Argomenti	L'esame in presenza è composto da 3 parti: 1) <u>test scritto</u> composto da domande a risposta chiusa (ossia 1 sola risposta di quelle presentate è vera). A positivo superamento di questa prova, 2) <u>"caso di studio"</u> : viene proposta una situazione reale, attinente alla specifica attività professionale, a cui il Candidato dovrà fornire una risposta appropriata A positivo superamento di questa prova, 3) <u>esame orale</u>, tramite videoconferenza	Per gli argomenti d'esame confrontare pag 3 *"Conoscenze, abilità e competenze associate all'attività professionale"* Il test scritto prevede 30 domande, con 3 risposte ciascuna ed è previsto un tempo massimo di 30 minuti (90 secondi per ogni domanda). Durante l'intero svolgimento della prova d'esame, il Candidato non può consultare alcun tipo di materiale didattico L'esito della prova è immediato. Il caso di studio prevede un tempo massimo di risposta di 30 minuti. Durante l'intero svolgimento della prova d'esame, il Candidato non può consultare alcun tipo di materiale didattico La risposta fornita dal candidato viene inviata al/i commissario/i, nominato da FAC CERTIFICA L'esame orale è volto ad approfondire eventuali incertezze riscontrate nelle prove scritte e/o per approfondire il livello delle conoscenze acquisite dal candidato ed è condotto da un commissario nominato da FAC CERTIFICA .Per tale prova è previsto un tempo massimo di 20 minuti
Criteri di valutazione	La valutazione massima ottenibile è di 100 punti, ed è data dalla sommatoria delle votazioni conseguite dal candidato nelle 3 prove d'esame La valutazione complessiva è positiva se la somma delle votazioni ottenute nelle tre prove (2 scritte e 1 orale) raggiunge almeno 60 punti, tenendo comunque presente che deve essere superata la soglia minima fissata per ogni prova: per la prima prova scritta 18 punti, per la seconda prova scritta 18 punti e per la terza prova orale 24 punti.	<u>Prima prova (test)</u>: viene attribuita una votazione massima di 30 punti: 1 punto per ogni risposta corretta, 0 punti per ogni risposta sbagliata o non assegnata <u>Seconda prova (caso di studio):</u> viene attribuito un punteggio massimo di 30 punti. <u>Terza prova (orale):</u> viene attribuita una votazione massima di 40 punti
Esito negativo esame	Nel caso di <u>non superamento</u> dell' esame il candidato potrà ripetere l'esame trascorsi almeno 3 mesi	La quota di iscrizione all'esame è da considerarsi per ogni partecipazione alla sessione
Esito positivo esame e Rilascio della certificazione	Il Candidato che dimostra il possesso di tutti i requisiti richiesti ed ha superato positivamente l'esame, viene proposto dal Direttore al Comitato di Delibera FAC CERTIFICA.	

	Il Comitato di Delibera valuta, sulla base di tutta la documentazione relativa al Candidato, il possesso dei requisiti e può riservarsi di accertare, ulteriormente, il possesso delle caratteristiche personali attraverso opportune tecniche (p.es. intervista, richiesta di documentazione aggiuntiva) ed eventuali informazioni da richiedere alle strutture presso cui, o per conto delle quali, il Candidato ha eseguito prestazioni. In tal caso, il Comitato stabilisce anche quali tempi e modalità siano necessari. Il Comitato di Delibera si riserva inoltre di valutare ulteriormente la congruenza tra la documentazione presentata dal Candidato, la valutazione effettuata dai commissari d'esame e la proposta di certificazione. Ad esito positivo della valutazione, il Comitato delibera per il rilascio della certificazione. La notifica dell'ottenimento della certificazione, unitamente alle modalità per la consegna di certificato, vengono comunicate al Candidato dal Direttore con l'ausilio del personale FAC CERTIFICA	